TRANSBORDER BIOMETRIC INFORMATION FLOW: LEGAL CHALLENGES TO PERSONAL PRIVACY AND THE NEED FOR PUBLIC DEBATE

By

Vanessa Díaz Rodríguez

Licenciatura en Derecho (Hons) (Lic., Universidad El Pedregal), Mexico

Maestría en Derecho (Hons) (Mtra., Universidad Anáhuac Del Sur), Mexico

Submitted in fulfilment of the requirements for a Degree of

Doctor of Philosophy

University of Tasmania

Faculty of Law

May 2014

DECLARATION OF ORIGINAL AUTHORSHIP

This thesis contains no material which has been accepted for a degree or diploma by the University or any other institution, except by way of background information and duly acknowledge in the thesis and, to the best of the candidate's knowledge and belief no material previously published or written by another person except where due acknowledgement is made in the text of the thesis, nor does the thesis contain any material that infringes copyright.

STATEMENT REGARDING PUBLISHED WORK CONTAINED IN THESIS

The publisher of the paper "Sistemas Biometricos en materia criminal: un estudio comparado" [Biometric Criminal Databases: a comparative study] in *IUS Revista* holds the material for section 2.3. The Biometric Systems Debate: Tracking History and part of Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow, and access to the material should be sought from the Instituto de Ciencias Juridicas de Puebla. The remaining no published content of the thesis may be made available for loan and limited copying and communication in accordance with the *Copyright Act 1968* (Cth).

STATEMENT OF AUTHORITY OF ACCESS

This thesis may be available for loan and limited copying in accordance with the *Copyright Act 1968* (Cth).

STATEMENT OF ETHICAL CONDUCT

"The research associated with this thesis abides by the international and Australian codes on human and animal experimentation, the guidelines by the Australian Government's Office of the Gene Technology Regulator and the rulings of the Safety, Ethics and Institutional Biosafety Committees of the University."

Signature.....

Date.....

ABSTRACT

This thesis is about the legal challenges posed by Transborder Biometric Information Flows (TBIF) and its impact on personal privacy and civil liberties in two contexts, immigration information flow and information flow in criminal databases. The thesis considers the role of national and international policy and regulation for TBIF in the contexts of immigration control and crime prevention. The examination of privacy and civil liberties is conducted within the framework of a comparative four countries study of Australia, Mexico, New Zealand and Spain. In comparison with the extensive international civil liberties literature, there is a significant absence of scholarly work on the legal impact of biometric technology, in general and on TBIF, in particular.

Chapter 1 set the framework for the research. The thesis explores the historical background to biometrics, its typology and purposes (Chapter 2) with a focus on TBIF applications. Before analysing the legal challenges of TBIF, the thesis maps the key players in the biometrics industry and their products and practices and finds a lack of industry ethical codes of practices and a need to improve self-regulation (Chapter 3). The four countries study framework examines the operation of TBIF in two specific contexts of immigration information flow and information flow in criminal databases (Chapters 4 and 5). The four countries study also informs the analysis of the legal challenges to personal privacy and data protection and civil liberties generally posed by TBIF in the two contexts of immigration and information criminal databases, at both the national and international levels (Chapter 6).

The thesis argues that all countries need to balance properly the public interests in national security with individuals' civil rights and liberties, when biometric systems are deployed and TBIF between and within jurisdictions are implemented. This balance, it is argued can be assessed and achieved with a due regard and reasoned approach to the application of the civil law proportionality and common law reasonableness tests (Chapter 7). This thesis concludes with proposals to achieve proper and proportionate levels of protection for TBIF and makes specific recommendations to amend privacy and data protection laws and reinforce existing privacy commissioner powers (Chapter 8)

EXPLANATORY NOTE

Biometrics is an evolving and dynamic area with regular technological and scientific developments occurring around the world. This thesis takes into consideration the latest technological, scientific, as well as legal developments as at 31 December 2013 in relation to the focus of this thesis on Transborder Biometric Information Flows (TBIF).

ACKNOWLEDGEMENTS

I am grateful to the *Instituto de Investigaciones Jurídicas de la UNAM* for their generous support, which enabled me to undertake a PhD program. I am also grateful to the *Consejo Nacional de Ciencia y Tecnologia (CONACYT)* and the *Instituto de Ciencia y Tecnología del Distrito Federal (ICyTDF)* for their overseas scholarships. I acknowledge the contribution of the University of Tasmania for awarding the *McDougall, Andrew Inglis Clark* and *Neasey* scholarships to support my empirical study trips.

I would like to express my very great appreciation to my primary supervisor, Distinguished Professor Don Chalmers for his valuable support, generous time, and advice. I would like to offer my special thanks to my co-supervisor, Associate Professor Rick Snell for his valuable and constructive suggestions during the planning and development of this research. I appreciate their patience in the writing of this thesis.

I would like to express my general gratitude to all the professors and public officers involved in my empirical research study for giving their time to meet with me and their comments, experience and knowledge. All their contributions were valuable for this thesis. Some of these people are specifically named and referred to in foot-notes and in the bibliography.

I am also grateful to a number of Law Staff for their enthusiastic encouragement and support: I thank Professors Margaret Otlowski, Gary Meyers, Dianne Nicol, Jeremy Prichard, Gail Lugten, Anja Hilkemeijer and Lynden Griggs. I would also like to thank the Law Library staff, Deborah Bowring, Christine Hurbugh, Carolyn Jarvis, Moira Mahony without whose support this research would not have been possible. My sincere thanks also go to the English Assist staff: Louise Oxley and Morag Porteous for their support. I acknowledge my fellow postgraduate friends for the stimulating discussions and support over the last three years.

My deepest gratitude to my family: my parents Carolina Aide and Alejandro and my sister Cynthia. They have always provided unwavering love and encouragement.

TABLE OF CONTENTS

ABBREVIATIONS

ABIS	Automated Biometric Identification System
ABTC	Asia Business Travel Card
AFIS	Automated Fingerprint Identification System
AIDC	Automatic Identification and Data Capture
ANSI	American National Standards Institute
APEC	Asia Pacific Economic Cooperation
APIS	Advanced Passenger Information System
APP	Advanced Passenger Processing
CCTV	Close Circuit Television
CFRUE	Charter of Fundamental Right of the European Union
CSL	Critical Skill List
DIAC	Department of Immigration and Citizenship (Australia)
DNA	Deoxyribonucleic acid
ECHR	European Court of Human Rights
EDNAP	European DNA Profiling Group
ENFSI	European Network of Forensic Science Institutes
ESS	European Standard Set
EU	European Union
FBI	Federal Bureau of Investigation
GCIM	Global Commission on International Migration
GOES	Global Online Enrolment System
GPS	Global Positioning system
ICT	Information and Communication Technologies
IACHR	Inter-American Court of Human Rights
ICAO	International Civil Aviation Organization
ICT	Information Communication Technology
INM	Migration National Institute (Mexico)
IOM	International Organization for Migration
ISO	International Organization for Standardization
ISSOL	Interpol Standard Set of Loci
IVSS	Immigration and Visa Support Solutions
MRTD	Machine Readable Travel Documents
NAFTA	North American Trade Agreement

NBS	National Bureau of Standards
NGO’s	Non-Governmental Organizations
NIST	National Institutes of Standards and Technology
OECD	Organization for Economic Co-operation and Development
PIRS	Personal Identification and Regulation System
PNR	Passenger Name Record
RFID	Radio Frequency Identification
SETRAM	Electronic System for Migration Procedures
SIS	Schengen Information System
STADNAP	Standardization of DNA Profiling in the European Union
TBIF	Transborder Biometric Information Flow
TDF	Transborder Data Flow

LIST OF FIGURES

CHAPTER 1.

TRANSBORDER BIOMETRIC INFORMATION FLOWS: LEGAL CHALLENGES

1.1. Introduction

Information and Communication Technologies (ICT) are providing rapid updates and advances in the speed of access, storage capacity and generation of data. Arguably, one of the most important advances in ICT has been the capacity to collect, store, process and exchange new types of data. Prominent amongst these new forms of ICT data are human genomic and biometric data. Human genomic data is revolutionising medical research as biometric data is shaping the security industry. The ICT industry has developed novel modes of data collection, storage and exchange of biometric information. There has been both intensification and a diversification in the use of these technologies. These exchanges of information can occur within countries or across borders.

Biometrics is not a new field of research and development[1]. What is new, however, in relation to biometrics, is the advances in automation to rapidly collect, store, process and exchange information; including, the capacity to build a large scale of networks and databases. This biometric technology has been intensified and diversified, and has penetrated into diverse areas of social interaction, from law enforcement, banking services, healthcare services, government social benefits and services, employment, immigration to even public transportation[2].

[1] For further details, see section 2.3. The Biometric Systems Debate: Tracking History
[2] For further details, see section 3.3. Biometric Systems Applications: Diversification into Different Fields

Aside from the technical aspects of this ICT revolution, there are considerable privacy and data protection issues involved with biometrics[3]. From a legal perspective, these ICT developments bring new challenges, limitations and problems. The deployment of biometric systems requires not only an informed public debate, but also the participation of citizens in these developments. These raises the question as how the deployment of biometric systems and Transborder Biometric Information Flows (TBIF) fit in democratic societies. To begin with, it can be observed that there must be legal responses to the deployment of biometric systems both nationally and to TBIF. These responses may range from self-regulation, to formal international cooperation and regulation. This thesis will focus on TBIF at the national and international levels in the two specific contexts of immigration information flow [4] and information flow in criminal databases[5] and will examine these areas in a comparative case study of four countries. This thesis does not consider the technical aspects of forensic DNA testing (deoxyribonucleic acid) in criminal investigations, prosecutions[6] nor does it consider the rapidly expanding use of databases for scientific research purposes. However, this thesis does present an overview of the expanding biometrics industry[7], but the market dominance of some specific companies in the industry are beyond the parameter of this thesis[8].

This thesis also examines some of the theoretical analyses of modern technology. In particular, this thesis focuses on rational-critical communication theory, which analyses how citizens come to know things and express general public opinion. Rational communication theory is a useful tool in addressing this rapidly developing biometric technology. The rational-critical communication theory work of Habermas,

[3] There is a distinguished characteristic between Civil Law countries and Common Law countries using the terms of “privacy” and “data protection”. This is further discussed in detail, see section 1.3. Country Profiles for the Comparative Study Component

[4] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[5] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

[6] General prosecutions, crime scene investigations, prosecution problems and evidence, see Chalmers D., *Genetic Testing in the Criminal Law*, (UCL Press, 2007).

[7] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

[8] For further details, see section 1.5. The Aim of the Research

Jasanoff, Villanueva and Ugalde is considered. This work analyses the right of citizens to access information with transparency, accountability and public debate.

This thesis considers the role of national policy and regulation in balancing the undoubted technical advantages of biometric systems with the critical civil liberty considerations. A four countries study examines the balance of public and private interest in the two contexts of immigration control and crime prevention. Balancing public interests with individual human rights is not contained with national boundaries. The deployment of biometric systems crosses border with TBIF that must be strictly scrutinised, supervised and regulated. The balance between public and private interests is addressed in Civil Law countries by the 'proportionality test'. The Civil Law "proportionality approach" is not unknown in countries with Common Law systems, such as England, New Zealand and Canada. Common Law countries usually express the "proportionality test" in terms of their traditional "reasonableness standard". This thesis will address the balance between public and private interests in the area of TBIF and the required level of privacy and data protection within the legal frameworks of the Civil Law proportionality test and Common Law reasonableness standard[9].

This introductory chapter sets out the fast evolving biometric industry and the role of privacy and data protection in the context of TBIF in immigration control and crime prevention. The examination of privacy and data protection is conducted within the framework of four countries comparative study component. This chapter also explains the methodology and aims in the specific context of TBIF in immigration information flow and information flow from national to international criminal databases. The research methodology and the reference system used is explained in this thesis. Finally, this chapter presents the research questions of the thesis.

[9] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

1.2. The Context of the Study: Deployment of Biometric Systems

This thesis analyses and assesses the current national and international frameworks for the deployment of biometric systems in the contexts of immigration information flow and information flow in criminal databases. There is a lack of critical legal and regulatory analysis of TBIF in general and in relation to immigration information flows and information flows in criminal databases in particular. This lack of legal regulatory literature is despite national governments implementing biometric systems for identification purposes[10]. This implementation of biometric technology has intensified and diversified in different fields over the last three decades[11]. Biometric systems pose challenges for individual privacy and civil liberties and this thesis analyses these challenges in two contexts, immigration information flow[12] and information flow in criminal databases[13]. Regulation has generally focused on national responses to these developments and has not involved public policy debates based on the introduction of the systems. Biometric systems involved a multiplicity of interests from politicians; supervisory authorities; the biometric industry itself; academic privacy groups; and, data protection activists. TBIF is a consequence of the implementation of biometric technology and transcends national borders; therefore, international cooperation is required for developing legal frameworks and common standards for law enforcement[14].

It is beyond the scope of this thesis to examine TBIF in all countries to understand all national responses. However, research for this thesis includes a four countries comparative study, limited to Australia, Mexico, New Zealand and Spain. A comparison between the biometric systems deployed in these countries aims to identify the common political agreements that are taking place internationally in relation to immigration control and crime prevention, especially in border controls and police co-operation. In the four countries study, an examination is conducted on

[10] For further details, see Chapter 2. Biometric Systems: What is Biometrics?
[11] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships
[12] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[13] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow
[14] For further details, see Chapter 8. Conclusions

the privacy and data protection legislation in each country and their legal frameworks for immigration control and biometric criminal databases. In addition, this thesis identifies the different emerging international and regional organisations that are developing regulation and standards for TBIF for different purposes, including immigration control and crime prevention. In the European Union, the EURODAC and the Schengen Information System (SIS) were identified and, in the Asia-Pacific Economic Co-operation (APEC) forum, the APEC Business Travel Card was identified. Globally, Interpol databases are significant in biometrics.

One country in the four countries study, Mexico, provides an illustrative example of both national regulation responses and the emerging international regulatory framework. At the national level in Mexico, the regulatory framework adopted for biometric profiles was a reaction to a specific situation which aroused much public opinion. This situation concerned irregularities during criminal investigations in Ciudad Juarez (Chihuahua)[15] about violence, murders and disappearances of women from the beginning of the 1990s. These investigations resulted in a prosecution case in the Inter-American Court of Human Rights, known as the "Cotton Field"[16] in 2009. Before this trail, Mexico responded to public opinion and enacted several laws that had the purpose to provide a clear signal to a vulnerable population about the need for greater public order. However, these laws failed to provide for an adequate level of protection and certainty. The irregularities continued at the time Mexico went to trial and the Inter-American Court decision found that Mexican processes had legal irregularities[17]. This Mexican event led to a deep reflection, not only about the collection, storage and process of biometric information but also about the purpose and use of TBIF and the proper balance of human rights.

[15] Ciudad Juarez is located in the north of the state of Chihuahua, on the border with El Paso, Texas. It is an industrial city –where manufacturing and/or assembly plants have flourished– and a place of transit for Mexican and foreign migrants. Therefore, various factors in Ciudad Juarez, such as social inequalities and the proximity of the international border, have contributed to the development of different types of organised crime, such as drug-trafficking, people trafficking, arms smuggling and money-laundering, which have increased the levels of insecurity and violence. *Gonzalez et. al. ("Cotton Field") v. Mexico* (2009) 113 Inter-American Court HR (ser C).

[16] Idem.

[17] The following legal irregularities were found: (i) an absence of information in the report about the discovery of the bodies; (ii) inadequate preservation of the crime scene; (iii) lack of rigor in gathering evidence and in the chain of custody of the evidence; (iv) contradictions and deficiencies in the autopsies; and (v) irregularities and deficiencies in the identification of the bodies, as well as in their improper return to the families. Ibidem, 333.

At the national level, the collection, storage and process of biometric information must be carefully considered when creating biometric profiles or databases. Countries should generally plan biometric profiles or databases as *exceptions* or restrictions to the right of privacy and data protection to the individuals whose data is involved in this case. The creation of biometric profiles and the inclusion to databases have constitutional legality so as to be applied in a constitutional democratic State[18]. Biometric systems should be reasonable and not excessive[19], and importantly guarantee respect for the rights of privacy and data protection. There should be a right to access, rectification, cancellation and objection to process personal information[20]. Measures should balance and reconcile, on the one hand, the practical aspects of the biometric systems with the individual and social interests in respecting the principles of dignity and human rights.

National legal rights to privacy and data protection are, however, not absolute rights. Privacy and data protection may be restricted by legislators and limitations on privacy and data protection are recognised in international instruments. These restrictions can be assessed by the "proportionality test", a legal tool used by most Civil Law countries but also implemented by international courts, such as the European Court of Human Rights[21] and the Inter-American Court of Human Rights[22].

---

[18] "Democracy implies the constant possibility of modifying anything, and this option is made legally feasible in the constitutional text. Thus, the Constitution shall be democratic, it shall allow and ensure democracy, and, also, be subject to democratic decisions. The constitutional State would then be, according to the words of Manuel Aragón, 'the intent of judicializing democracy and the Constitution, the way in which such pretention is carried out'. The people are the author of the Constitution. So, constitutionalism and democracy combine in order to create a government system known as constitutional democracy". Nava Gomar, Salvador Olimpo, "El Estado constitucional: sinonimia positivizada entre Constitución y democracia (triple relación)" (2003) *Anuario de Derecho Constitucional Latinoamericano,* p. 14.

[19] It is important to recall an event that occurred in September 2000, when the former British Prime Minister Tony Blair announced the creation of a genetic record of every criminal –about 3 million citizens that were suspected of crimes or offences– within a 3-year term. He reflected his concern for public opinion that seemed to consider his public order initiatives were "weak". Mackey Neil, "Blair's DNA crime database plan 'dangerous and flawed'", *Sunday Herald*, (Glasgow, United Kingdom), 3 September 2000, 2.
http://www.shirleymckie.com/documents/Herald3.9.00.pdf (17/12/2012) Nevertheless, the measure raised protests from civil rights organizations due to facts such as the possibility of taking DNA samples from persons that committed traffic violations.

[20] These rights are known ARCO rights or Habeas Data. Kuschenwsky, Monika (ed.), *Data Protection and Privacy Jurisdictional Comparison* (Thomas Reuters, 2012).

[21] European Court of Human Rights http://www.echr.coe.int/echr/homepage_EN (19/02/2013)

This test is about the strict justification for any interference in human rights by law. This thesis considers the Civil Law "proportionality test" and its counterpart the "reasonableness standard" in Common Law countries, as a means to achieve the required balance between human rights and public interests[23].

The creation of biometric databases involved with TBIF for immigration control and crime prevention must have justification and constitutional legality. The comparative four countries study identified important broad convergences, and some asymmetries in the modes of data collected, updated, retrieved and exchange information, in the two contexts of immigration information flow and information flow in criminal databases[24].

1.3. Country Profiles for the Comparative Study Component

1.3.1. *The four countries selected*. The countries selected for the four countries study, as stated before, are an illustrative attempt to identify national regulation as responses to the rapidly development of biometric technology. The countries selected for the comparative study component are: Australia, Mexico, New Zealand and Spain. The selection was made for the following reasons:

- The four countries are deploying biometric surveillance technology.

- The four countries have "functional borders" where is a requirement for a formal travel documentation to ensure legal entry[25].

- The four countries exchange information about immigration and criminal records.

---

[22] Inter-American Court of Human Rights http://www.corteidh.or.cr/index.cfm?&CFID=1699709&CFTOKEN=26178292 (19/02/2013)

[23] For further details, see section 7.4. The Principle of Proportionality: Legitimate Restrictions on Privacy and Data Protection

[24] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

[25] Weber, Leanne and Pickering Sharon, *Globalization and Borders. Death at the Global Frontier,* (Palgrave MacMillan, 2011), p. 4.

- The four countries are Interpol member countries.

- The four countries examined represent the Civil Law[26] (Mexico and Spain), and the Common Law[27] (Australia and New Zealand) systems.

- Australia, Mexico and New Zealand are country members in Asia-Pacific Economic Co-operation (APEC) whereas Spain is member of the European Union. The other three countries interact with the European Union.

- The four countries have concerns about illegal immigration.

- Legislation is the major source of law in Australia[28], Mexico, New Zealand[29] and Spain[30]. The two Civil Law countries illustrates the data protection legislation whereas the two Common Law countries exemplify the privacy legislation.

- From a practical stand point of view, these countries were selected on the basis of the ability to access to research resources by familiarity with Spanish as a first language for Mexico and Spain and English as second language for Australia and New Zealand.

This comparative study component was undertaken to assess the national regulatory framework and also to determine the international regulatory framework as a response of common political international agreements regarding the fields of immigration control and crime prevention. A comparison between these countries indicates how Civil and Common Law countries face the challenges involved in the

[26] The Civil Law system is both the older and the more widely distributed legal tradition. The date of its origin is 450 B.S., the date of publication of the Twelve Tables in Rome.
[27] The date commonly used to mark the beginning of the Common Law system is A.D. 1066, when the Normans defeated the defending natives at Hastings and Conquered England.
[28] Hall, Kath and Macken, Claire, *Legislation and Statutory Interpretation*, (Lexis Nexis Butterworths, 2nd ed., 2009), p. 2.
[29] Mulholland, R.D., *Introduction to the New Zealand Legal system*, (Butter Worths, 1976), p.1.
[30] "The amount of legislation and the degree of authority of legislation are not useful criteria for distinguishing civil law systems from common law systems". Merryman, John Henry and Perez-Perdomo, *The Civil Law Tradition. An Introduction to the Legal systems of Europe and Latin America,* (Stanford University Press, 3rd ed., 2007), p. 27.

deployment of biometric systems. In looking at the national and international framework the theoretical context of the deployment of biometric systems is considered as well as national approaches of political and public debates surrounding such systems.

1.3.2. *Four countries study.* It is worthwhile to set out brief country profiles. Australia and Mexico operate as federal systems whereas New Zealand and Spain are unitary. However, the Spanish government acts *de facto* as a federal system, with the central government in Madrid affording some limited delegation to local regional bodies[31]. These four countries have important similarities: for example, all are multicultural societies with a range of ethnic groups represented; their branches of government and administrative divisions overlap and each enjoys universal suffrage. However, Australia is the only one of the four countries that has in force a system of compulsory suffrage. The differences among the four countries may be more obvious in, for example, population, geographic area (sq km)[32], currency, gross domestic product, legal system and language.

The four countries examined differ importantly in their legal, cultural and political traditions; this is also the case even with Spain and Mexico despite a number of shared traditions. Mexico´s Civil Law system is the result of different influences. Before the Spanish conquest, there was an indigenous customary law embodied in Codices. During colonial times special laws were enacted called “Laws of the Indies”. Later, the Spanish Civil Law created a highly formal body of law, including a specific collection of laws, but also recognition of customs or accepted “legal” indigenous practices. After 200 years of Spanish domination, Mexico began the Independence movement on September 16th, 1810, and this ended, officially on September 21st, 1821. Mexico enacted its first *Civil Code*, in 1870, influenced by the French, *Code Napoleon*. The development of Mexican commercial law drew heavily on Italian law. Mexico's legal system was also influenced by the United States’ constitutional law; mixing the system of “checks and balance” and judicial review of legislative acts in

[31] Merryman, John Henry and Perez-Perdomo, *The Civil Law Tradition. An Introduction to the Legal systems of Europe and Latin America,* above n 30, p. 58.
[32] Australia 7,692,024 sq. km., Mexico 1,964,375 sq. km., New Zealand 268,680sq km and Spain 505,988 sq. km.

the Mexican Constitution[33]. The following figure presents the convergences and differences between Australia, Mexico, New Zealand and Spain in relation to selected indicators.

Figure 1. National Profiles[34]

	Australia	Mexico	New Zealand	Spain
Capital	Canberra	Mexico City	Wellington	Madrid
Population	22,683,600	112 336 538	4,453,062	46,815,916
Area (sq km)	7,692,024	1,964,375	268,680	505,988
Major Language	English	Spanish	English	Spanish
Currency	Australian Dollar	Mexican Peso	New Zealand Dollar	Euro
Ethnic Groups	European 92% Asian 7% Aboriginal and other 1%	Mestizo 60%, Indigenous 30%, European 9%, other 1%	European 69.8%, Maori 7.9%, Asian 5.7%, Pacific islander 4.4%, other 0.5%, mixed 7.8%, unspecified 3.8%	composite of Mediterranean and Nordic types
Government Type	Parliamentary democracy	Federal democracy	Parliamentary democracy	Parliamentary monarchy
Administrative Divisions	6 states and 2 territories	31 states and 1 federal district	16 regions and 1 territory	17 autonomous communities and 2 autonomous cities
Constitution	1900 Constitutional Monarchy	1917 Constitutional Republic	1986 Constitutional Monarchy	1978 Constitutional Monarchy
Legal System	Common Law	Civil Law	Common Law	Civil Law
Suffrage	18 years of age; universal and compulsory	18 years of age; universal and compulsory	18 years of age; universal	18 years of age; universal
Branches	Executive, Legislative and Judicial	Executive, Legislative and Judicial	Executive, Legislative and Judicial	Executive, Legislative and Judicial
GDP	3.4	3.9	3.0	-1.4

Source: Information obtained from different websites: Australian Bureau Statistics, Instituto Nacional de Estadistica y Geografia (Mexico), Statistics New Zealand, Instituto Nacional de Estadistica (Spain), the World Bank.

1.3.3. *Privacy and data protection.* There is a significant asymmetry between these four countries in the use of the term "privacy". The terms "privacy" and "data protection" are not synonymous in these countries[35]. In general terms, the right to privacy is an essential right for the individual which deserves the highest respect as guarantee for other freedoms. In the Civil Law tradition approach, the right to data protection is what characterises a private life (right), understood as the right to be

[33] After this Independence war, Mexico had a period of wars called "Interventions" against Spain, France and the United Sates (U.S.) that affected the development of its legal framework, as well as its economy and geographical territory. These "Intervention wars" were: first against Spain in 1829, the second was against France from 1838 to 1839, the third with the U.S. from 1846 to 1848, a fourth was against France from 1862 to 1867, then came another against the U.S. in 1914 and finally another again with the U.S. in 1916.

[34] For a complete appreciation of Figure, see Appendix A. National Profiles Table

[35] Cooper's works are a distinctive and stand out by the author's analysis of the terms "privacy" and "data protection". Cooper concluded that although these terms are used in different jurisdictions, both terms are essentially synonymous. Nevertheless, this thesis does not share Cooper's conclusion. Cooper, David M., "Transborder data flow and the protection of privacy: the harmonization of data protection law", (1984) 8 *Fletcher Forum*, p. 339.

protected from illegitimate or legitimate but unwanted intrusion[36]. The right of data protection seeks to preserve privacy and confidentiality in the collection, management and transmission of personal information. In Civil Law countries the recognition of "control of what has been collected about personal life" is known as "informative self-determination". So in Civil Law countries, the "informative self-determination" right recognises the person as the owner of his or her personal information generated or stored by governments[37]. Control, here, is related to the possible exchange of personal data or the subsequent automated use of this personal information. An example of this is provided by the electronic health record, where a patient is the owner of the information recorded, but the public health provider or centre creates, maintains the records and stores the person´s medical information. The patient, in this case, has the right to access to his or her own electronic health records and to challenge any disclosure or subsequent use of his or her records.

The term "privacy" is used in a broad sense in Common Law countries to refer to the protection of an individual's personal life, including personal data, whereas the term "data protection" in Civil Law countries has a narrow meaning to refer to specific personal information (personal data)[38]. This is illustrated by the article 18 of the Spanish Constitution which uses the Spanish word "intimidad". The literal translation of this, in English is "intimacy" and the Spanish law refers to the protection of individuals' personal life. The Spanish and Mexican legislation refer to data protection[39].

1.3.4. *Proportionality*. A distinguishing characteristic emerged in the comparative study component between the four countries with respect to "principle of proportionality". The 'proportionality test' is a means to find the proper legal balance between the individual rights and the public interest. This legal balance is achieved,

[36] Gozaíni, Osvaldo Alfredo, *Derecho Procesal Constitucional, Hábeas Data, Protección de datos personales*, (Rubinzal-Culzoni Editores, 2001).
[37] Idem.
[38] Idem.
[39] This also can be illustrate by the Ibero-American countries use the terms "informative self-determination" or "*habeas* data" to refer to specific characteristics of procedures related to data protection. Ibero-America is a term used to refer collectively to Spain, Portugal and countries in the Americas that were formerly colonies of Spain and Portugal.

in Civil Law countries with the 'proportionality test'. Arguably, this distinction is not so significant between Civil Law countries; Common Law systems, such as New Zealand, Canada, and England; and, mixed legal systems such as South Africa. In these countries, the "proportionality test" and the legal balance is achieved by the "reasonableness standard"[40].

The appropriate balance between the deployment of biometric systems for public purposes and individuals' privacy and data protection rights is a major focus of this thesis. So too, is the appropriate legal framework for standards of TBIF by reference to the proportionality test.

1.4. Hypothesis

The major hypothesis of this thesis is that the public purposes, use and deployment of biometric information in Transborder Biometric Information Flow (TBIF) may undermine individuals' civil liberties. TBIF uses automated techniques which facilitate the linkages of many databases nationally and internationally. These automated flows of information may breach in established rights of privacy and data protection.

The main arguments in relation to this hypothesis are as follows:

a) The establishment and deployment of national and also international biometric databases are measures that limit the individual rights of privacy and data protection, which are legally recognized and respected in democratic societies. Linkages of these databases must be legally controlled. This thesis acknowledges that there are some circumstances in which the State may circumscribe human rights. However, "these circumstances" should be specific, limited and justified by reference the principle of proportionality and the reasonableness standard.

[40] For further details, see section 7.4. The Principle of Proportionality: Legitimate Restrictions on Privacy and Data Protection

b) The biometric industry itself should establish proper and published standards of self-regulation. Self-regulation is a priority because a basic mapping of this expanding industry does not reveal an industry commitment to ethical and privacy practices where the industry itself enjoys a position of, market dominance[41]. The thesis assesses a basic map of this industry to inform the national responses for regulation.

c) Public policy surrounding the implementation and deployment of biometric databases and TBIF should be openly debated to ensure proper levels of transparency and public accountability. This argument flows directly from research and theoretical frameworks proposed by Jasanoff in her works on "civic epistemology" and by Habermas in his ideas on the "public sphere", which are mentioned in this chapter[42].

d) TBIF and the subsequent chain of linkages to other databases involving different agencies from different fields nationally and internationally, challenges and undermines individuals privacy and data protection rights. International privacy and data protection regimes should ensure that personal information should only be collected for a specific purposes and be used solely for legitimate purposes that can be scrutinise, challenge and supervise.

e) Misclassification of data can occur in TBIF and can result in misclassification of immigrants as illegal immigrants or misclassify types and levels of offenders or people listed on these databases. Problems of misclassification are focus in this thesis.

[41] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships
[42] For further details, see section 1.8.3. Theoretical Approaches

f) The “proportionality test” in Civil Law and its counterpart the “reasonableness standard” in Common Law countries can address the legal challenges for TBIF related to privacy and data protection rights. The proper balance between public interests and individual human rights are focus in this thesis[43].

1.5. The Aim of the Research

The aim of the research is to examine and assess the legal challenges, limitations and concerns of TBIF in two contexts, immigration information flow and information flow in criminal databases[44]. Within this aim, the research considers and assesses national and international responses for an adequate level of legal protection for TBIF in these two contexts.

With this major aim, the thesis examines the diversification and intensification of the rapidly developing biometric industry by mapping key industries, products and partnerships. In addition, an empirical four countries study was undertaken to identify and assess officially available information about biometrics related policies and regulations that are not accessible online. This four countries study identified policies and included interviews with officials to understand towards international policies[45].

The thesis includes proposals for practical and achievable solutions for addressing TBIF challenges in the two contexts of immigration information flow and information flow in criminal databases but also proposes greater public debate, transparency and accountability in relation to the development of this technology.

[43] For further details, see section 7.4. The Principle of Proportionality: Legitimate Restrictions on Privacy and Data Protection

[44] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

[45] These interviews were conducted in accordance with formal University of Tasmania Ethics approval, reference H0012013 of 20/08/2014. The information collected in the four country study was explanatory and did not breach any secrecy or confidentiality, the information was helpful because it identified official political processes and policy making procedures and was indicative of future directions for policy developments.

1.6. Limitations of the Research

A key limitation in the research for this thesis was the lack of traditional scholarly sources of research and writing of this specific area of TBIF. Whilst there is a body of accumulated literature about cross-border economic or business transactions, there is not a substantial body of scholarly work on the biometric industry in general or on TBIF in particular. There is published work on the technical and historical development of biometric systems[46], but only a handful number of published work dealing with the specific legal and regulatory issues involved in biometrics and privacy[47].

1.7. The Significance of this Study

The research for this thesis is significant for the following reasons:

- The thesis contributes to an understanding of the developing study of biometric technology and industry and the relative lack of official self-regulation for TBIF.

- The research contributes on the wider public debate on the need of transparency and accountability surrounding the introduction and the deployment of TBIF in the contexts of immigration control and crime prevention.

[46] Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, (W.H. Freeman and Company, 1973); Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*"* (1999) 13(3) *International Review of Law, Computers & Technology* 337-363; Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000); Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003) and Bolle, Ruud M., et. al., *Guide to Biometrics*, (Springer, 2003).

[47] Van Der Ploeg, Irma, "Biometrics and Privacy: A note on the politics of theorizing technology" (2003) 6 *Information, Communication & Society* 85-104; Lyon, David, *Identifying Citizens: ID Cards as Surveillance* (Polity, 2009); Lyon, David and Bennett, Colin (eds.) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (Routledge, 2008); Epstein, Charlotte, "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders" (2007) 1 *International Political Sociology* 149-164.

- The thesis provides a limited map of the biometric industry and identifies the need for a system of self-regulation in the biometric industry.

- The thesis identifies deficiencies on TBIF in specific circumstances, such as immigration control and crime prevention, and makes specific proposals to address these concerns.

- The thesis identifies the need for a greater international cooperation for a TBIF. Transborder Data Flows have been on the international agenda since the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[48] in 1980 and the movement of data protection laws that started to emerge, especially in the European Union and the United Sstates of America[49]. Two additional OECD reports were produce in 2004 on biometrics recognition technology[50] and in 2006 on cross-border enforcement of privacy laws[51]. These reports focused on transborder financial data and did not resolve the issue of TBIF.

- This thesis contributes to the development of national and international framework with practical and achievable proposals that address TBIF privacy and data protection within the legal framework[52]. These proposals may influence legislative policy and decision-making on the deployment of biometric systems in different countries.

[48] Economic Cooperation and Development's (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows or Personal Data* (1980).
[49] It is possible to identify academic work on the topic of TDF since the 1970s and 1980s, where the main characteristic of these works are discussions on personal data transferred for business transaction purposes.
[50] OECD, *Biometric-based Technologies*, Report 101 (2004) http://dx.doi.org/10.1787/232075642747 (22/08/2012)
[51] OECD, *Report on the Cross-Border Enforcement of Privacy Law,* Report 121 (2006) http://dx.doi.org/10.1787/231304814207 (23/12/2012)
[52] For further details, see section 7.5. Recommendations to Address Legal Framework for TBIF

1.8. Research Methodologies and Theoretical Approaches

Different theories and methods including an empirical study of the rapidly developing industry, traditional legal methods of statute and cases analysis (both Common Law and Civil Law) and a comparative methodology were incorporated into this thesis. The following specific methods and theories were used for the research.

1.8.1. *Empirical*. This method was employed in two different stages of the study. First, through websites searches which, helped to draw a general map of the biometric industry identifying key industry players, products and partnerships[53].

Second, semi-structured face-to-face interviews with academics and public officials in the four countries were applied to the baseline mapping of the industry to complement the extent of biometric use and identify the emerging policy development in relation to TBIF.

These semi-structured face-to-face interviews with academics and public officials in the four selected countries[54] were conducted with under an Ethics Approval with a Minimal Risk Ethics Application from the Tasmania Social Sciences HREC.

1.8.2. *Social Science Methods*. The thesis made use of the following methods:

- Deductive: the starting point is the relationship between the established right to privacy and data protection, the right to access to personal information and their connection with security and police co-operation. The research considers the right to privacy and data protection as a fundamental freedom for the individuals, an essential pillar in the construction of constitutional democratic States.

[53] For further details, see Appendix D. List of Companies in the Biometric Industry (Complete Table)
[54] For further details, see Appendix J. Interview Questions and Interviewees

- Inductive: the point of departure in the research is the analysis of local criminal law and the initiative for international police co-operation in order to identify the reasons for undermining privacy and data protection and subsequently fulfil the purpose. The research also analysed immigration laws and criminal databases frameworks.

- Analytical: the individual right to access to one´s own personal information is set apart from the right to data protection. A theoretical framework was elaborated for the purpose of establishing a balance between civil liberties as a necessity in a democratic society; and the need to protect security and public interests. The transmission and preservation of biometric information in relation to the criminal offences in Federal or National Criminal Codes are identified and analysed in the four countries examined.

- Synthetic: with this method, the research detected the causes of restrictions to the right to privacy and data protection in the four countries examined.

- Comparative: the research identified how the four countries, with their legal and public ethics value systems, have implemented biometric systems and regulate the universal principles of dignity, confidentiality and privacy in their biometric databases imply, as well as how legal conflicts are solved.

- Historical: the research analyses the precedents of biometric technology.

1.8.3. *Theoretical Approaches*. The following approaches were applied for the study:

- Modern technology theory. This theory is about the theoretical analyses of modern technology were used, particularly the “systemic understanding of co-production (spread of knowledge)” and “rational-critical communication (public debate)” theories of Sheila Jasanoff (civic epistemology) and Jürgen Habermas (public sphere) Ernesto Villanueva and Luis Carlos Ugalde who

uphold the importance of public debate, transparency and public accountability[55].

- Human Rights theory, especially on the rights to privacy and data protection. The works of Georgina Battle, Carlos Ruiz Miguel, Alan Westin, Samuel D. Warren, Louis D. Brandeis, Irma van Der Ploeg, Ruth Gavison and Lee A. Bygrave are referred to serve as the foundations for the content of the rights to privacy, data protection and right to access to personal information.

- Civil Law Constitutional law theory rests upon the conceptual framework of a constitutional democratic State and considers that its foundations lay upon two fundamental pillars: the recognition of the public freedoms as a limitation to public power, and, the establishment of internal and external controls for public administration.

  The "power of reform" (legislative power) should not unduly infringe upon the content of individual rights by imposing limitations for political interests because rights are already recognized and guaranteed constitutionally. It would be remarkably difficult for a citizen to oppose for the collection of biometric information when the request of information has been legitimate by the government, where previously this request is found in the legal framework and not to win elections, for example. But, then, following this line of argument, citizens should demand continuity of privacy and data protection to countries where biometric information has been exchanged without regulation and legislative scrutiny[56].

[55] An important characteristic of "public sphere" and "civic epistemology" is that information should be complete and in a plain language to enable citizens to participate in a democratic society. In addition, through public policy debates and participation of citizens it is possible to legitimise not only the deployment of technology but also public policies related to this type of technology.

[56] It mentions as elsewhere argued in this thesis the concept of a democratic constitutional State through the work of Águila, Rafael del, *Manual de Ciencia Política* (Editorial Trotta, 5th ed., 2008); Aragón, Manuel, *Constitución, Democracia y Control*, (Instituto de Investigaciones Jurídicas de la UNAM, 2002); García De Enterría, Eduardo, *La Constitución como norma y el Tribunal Constitucional*, (Editorial Civitas, 2006); Nieto, Santiago, *et. al.*, *Control externo y responsabilidad de los servidores públicos del Distrito Federal,* (UNAM, 2005); Nino, Carlos, *La constitución de la democracia deliberativa*, (Gedisa, 1997). Pérez Luño, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución,* (Tecnos, 2003); Sartori, Giovanni, *Homo Videns, la sociedad teledirigida,*

- International Public law theories and International treaties, conventions and regional agreements in relation to human rights and biometrics technology were analysed in this thesis, as well as their interpretations through the resolutions form international tribunals, particularly the European Court of Human Rights (ECHR) and the Inter-American Court of Human Rights (IACHR). The work carried out by the Asia-Pacific Economic Cooperation (APEC) was also considered, as was that of the European Union (EU) and Organization for Economic Co-operation and Development (OECD) for the purpose of studying the corresponding considerations or conflicts for the implementation of the regulations on this issue.

1.9. Reference System

The comparative approach adopted for this thesis covers four jurisdictions (Australia, Mexico, New Zealand and Spain) and involved analysis and comparison of different sources in legislation, protocols, reports, cases, guidelines, books and academic articles, across these jurisdictions.

A significant feature is that both Australia[57] and New Zealand[58] have official guidelines regarding legal citations for academic research, but neither Mexico nor Spain has such regulation. In these two countries, each academic institution sets its own editorial criteria for legal citations. This thesis follows the "Guidelines and Criteria of the National Autonomous University of Mexico"[59] when citing from Mexican or Spanish sources.

(Taurus, 2004); Vega García, Pedro de "Significado constitucional de la representación política" (1985) 44 *Revista de Estudios Políticos* 53-74.

[57] Australian Guide to Legal Citation http://www.library.uq.edu.au/endnote/aglc/aglc3_ENX4.pdf (22/01/2013)

[58] New Zealand Law Style Guide http://www.lawfoundation.org.nz/style-guide/index.html (22/01/2013)

[59] Marquez Romero, Raul (ed.) *Lineamientos y Criterios del Proceso Editorial*, (UNAM, 2008) http://www.juridicas.unam.mx/publica/critedit/critedit.pdf (22/01/2013)

Therefore, both the bibliography and footnotes follow the Australian Guide to Legal Citation. However, it is noted that in the case of legislative material from both Mexico and Spain, some information was added, such as the publication date and latest revision published in both the Official Journal of the Federation (DOF) (Mexico) and in the Official Gazette (BOE) (Spain), as well as the official website for easier and clearer reference. Such information is generally translated from original Spanish.

1.10. Appendices

This thesis includes detailed appendices on information relevant of this thesis [on Biometrics Typology, in appendix B; the Schengen Information System, in appendix F; the Prüm Convention, in appendix G; and, National Immigration Policy, in appendix H]. This information is included in appendices rather than in the body of this thesis to avoid breaking the flow of the arguments. Each appendix has been cross referenced it in the body of this thesis.

1.11. Research Questions and Overview of the Thesis

The thesis considers the following research questions:

What is biometrics and what are the key legal issues involved in biometric systems?

In Chapters 2 and 3, the thesis provides the context for biometric systems. Chapter 2 briefly traces the most important events in the history of biometrics, its definition, typology and conditions. This includes a critical review of how biometric systems operate and the various uses of biometric technology. Chapter 3 discusses the biometric industry; mapping the context of the biometric industry, its importance and the development, diversification and intensification of this technology. The chapter identifies key companies, products and partnerships behaving different in each country studied. This chapter also discusses ethical practices in the biometric industry and the necessity for self-regulation.

What are the legal issues in biometric systems related to immigration and criminal databases?
This question includes the related questions of How do countries collect, retrieve, store and exchange information? How are the approaches of the implementation of biometric systems between the four countries examined? How do we learn and know about biometrics? And who spreads the knowledge of biometrics?

In Chapters 4 and 5, the thesis examines privacy and data protection by collecting, retrieving, storing and exchanging biometric measurements for immigration control and border security purposes. The thesis also considers the circumstances in which the State legally and reasonably limit and challenge individuals' privacy and data protection rights. Chapter 4 discusses controversies about the proper balance between State powers and individuals rights in relation to the modes of data collection and the capacity for such data to be collected, updated, retrieved, analysed and exchanged in the context of immigration control. The governance and regulatory systems are analysed for immigration using a comparative methodology. Chapter 5 examines criminal databases and the actual collection methods for DNA and biometric information. This chapter analyses the actual systems for the exchange of information and linkage with international biometric databases. The research considers Interpol's databases as the best practice for biometric criminal databases.

How does cross-border biometric data flow?
This question includes the related legal questions of what are the legal challenges at national and international level in relation to TBIF? Are the legal frameworks proportional between the public interest and human rights?

In Chapters 6 and 7, the thesis contains analysis of the central research questions in relation to the legal challenges to the balance between the legitimate interests of the State in the protection of their citizens balanced against individual privacy and data protection rights. Chapter 6 examines these legal challenges at national level in the context of immigration information flow and information flow in criminal databases. This chapter considers the challenges of TBIF within the framework of the four

countries study. Chapter 7 discusses TBIF at the international level with an examination of the official and semi-official international organisations. This chapter assesses the developing international regulatory framework against the national level to assess, using comparative methodology, the adequacy and effectiveness of national privacy and data protection legal framework. Importantly, this chapter includes practical and achievable proposals for revisions and improvements in the legal framework for TBIF.

What are the findings and the conclusions of this research?

Chapter 8 presents the findings of the research and the conclusions of this thesis. This chapter acknowledges the rapidly developing biometric industry diversifying into different field with limited regulated intervention and a lack of self-regulation. The chapter examines the actual emerging international regulatory framework for TBIF in immigration control and crime prevention contexts. The chapter identifies asymmetries and common legal concerns in immigration information flow and information flow in criminal databases for TBIF in the four countries study. The chapter proposes a practical and achievable solution for an effective TBIF legal framework relying on privacy and data protection regimes.

CHAPTER 2.

BIOMETRICS SYSTEMS: WHAT IS BIOMETRICS?

2.1. Biometrics Critical Review

The history of biometrics reveals a development process that has been *ad hoc*, led and initiated by scientific breakthroughs and technological innovations. Deployments of biometric systems have often occurred well in advance of regulatory consideration by policy makers and law reformers, and public discussions about the systems have been limited and retrospective. Furthermore, in recent decades, biometric systems have expanded and diversified rapidly and the intensification of their impact upon privacy and data protection, accountability and citizen-state relations have not been fully explored, understood or incorporated into an informed, considered and systematic approach to regulation.

Whilst not all biometric systems have an equal impact upon areas like privacy and civil liberties those systems that focus on identification and authentication purposes are particularly important areas. The collection, storage, retrieval and actual use of biometric information in areas like Transborder Biometric Information Flows (TBIF), especially immigration information flow[1] and information flow in criminal databases[2], needs far more extensive scrutiny, debate and attention especially from those outside the biometric industry[3]. An overview on the history of biometrics and its development reveals little attention given to regulation and/or the balancing of civil liberties and the public interest. The dynamic nature of recent developments, covered in this thesis, has intensified the necessity to find ways to ensure a full

[1] For further details see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[2] For further details see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow
[3] For further details see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

public discussion of these developments. A necessity for all four countries featured in this thesis.

The failure to foster or develop a robust public discussion about these developments, especially those at the centre of this thesis, and the relative exclusion, or marginalisation of various interests from participating in the development of regulatory frameworks is a major deficiency. In terms of a Jasanoff and Habermas analysis the key problems are the lack of: public debate, transparency and scrutiny. The deployment of biometric technology needs to be surrounded by transparency, accountability, citizen engagement and collaboration of multiple interests, such as civil society, biometric industry itself and supervisory authorities. According to Jasanoff and Habermas, governments focus more on the particular outcome rather than on the process to achieve that outcome and forget that it is the process that confers legitimacy[4].

The significance of a brief historical review is that it demonstrates some constant themes. First, the focus of most of the key authors who have written about biometrics since the 20th century onwards has been to focus on biometrical knowledge its development, application and reliability. Any discourse about the relationship between citizens, State and emergence biometric developments have been rare or non-existent. Some authors have discussed the legal impact of biometrics on privacy and data protection[5], yet they have not focused in extension on regulation, industry self-regulation or the necessity for public debate. A by-product of much of this

[4] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* (Princeton University Press, 2007) and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Einaudi, 1980).

[5] Van Der Ploeg, Irma, "Biometrics and Privacy: A note on the politics of theorizing technology" (2003) 6 *Information, Communication & Society* 85-104; Bygrave, Lee, "Privacy Protection in a Global Context –A Comparative Overview" (2004) 47 *Scandinavian Studies in Law* 319-348; Bygrave, Lee, "The Place of Privacy in Data Protection Law" (2001) 24(1) University of New South Wales Law Journal http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (20/12/2013); Lyon, David, *Identifying Citizens: ID Cards as Surveillance* (Polity, 2009); Lyon, David and Bennett, Colin (eds.) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (Routledge, 2008); Epstein, Charlotte, "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders" (2007) 1 *International Political Sociology* 149-164.

authorship is a technical literature of limited accessibility that compounds the largely "industry" focus shown in Chapter 3[6].

This chapter traces the historical background of privacy and presents a general introduction of biometric systems. Research was undertaken through traditional sources to draw a general sketch of the technical literature. This research uncovered little traditional scholarly sources of research with multidisciplinary approaches and little to spread the knowledge. This chapter draws the relationship between biometric systems and the rights to privacy and data protection. It discusses the most popular physical and behavioural characteristics, including DNA for biometric systems and the creation of biometric profiles through the purposes and limitations of biometric systems. Finally, this chapter identifies the necessity for an informed public discussion of biometrics' knowledge.

2.2. Comments on the Articulation of Biometrics Knowledge

The well-established line of technical literature related to biometric systems explains its origin and typology. These authors explain how biometric profiles are created, how these systems work, their purposes and their applications[7]. Nevertheless, these authors do not explain the relationship to or handling of privacy in terms of biometrics and are largely written for a technical audience.

[6] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

[7] Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, (W.H. Freeman and Company, 1973); Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*"* (1999) 13(3) *International Review of Law, Computers & Technology* 337-363; Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000); Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003); Bolle, Ruud M., et. al., *Guide to Biometrics*, (Springer, 2003).

Historical, social and political factors have shaped the definition of biometric systems. An interesting perspective is developed from sociology, in the articulation of biometric knowledge represented by Epstein[8] and Lyon[9] whose works explain how biometrics is used in a surveillance society.

The concept of biometric systems is moving towards empowering society, global communication, information technologies and the biometric industry, where all these actors are interrelated in this technology. According to the theoretical analyses of modern technology, it is essential to understand the importance of multidisciplinary approaches in the literature on biometric systems in order to know on which side interests are tipping the balance[10].

Jasanoff defines "civic epistemology" to be "the systematic practices by which nation´s citizens come to know things in common and to apply their knowledge to the conduct of politics"[11]. Habermas defines "public sphere" as the "first of all a realm of our social life in which something approaching opinion can be formed where access is guaranteed to all citizens"[12].

If science and technology are considered as instruments of social progress and personal liberation[13] why cannot citizens, in constitutional democracies, access easily to public information regarding the deployment of biometrics. The preliminary expectation was to find traditional scholarly sources of research with multidisciplinary approaches; however, there is not a substantial body of scholarly work on the biometric industry or on Transborder Biometric Information Flows (TBIF)[14] in comparison with the extensive privacy and data protection literature, where scholarly work covers different approaches its many challenges and limitations.

---

[8] Epstein, Charlotte, "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders," above n 5.
[9] Lyon, David, *Identifying Citizens: ID Cards as Surveillance,* above n 5.
[10] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[11] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4.
[12] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[13] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4.
[14] For further details, see section 1.5. The Aim of Research

This lack of literature and the lack of multidisciplinary approaches directly affect the central role of civic engagement in the articulation of biometric knowledge. According to Jasanoff:

> "[D]emocratic theory cannot be articulated in satisfactory terms today without looking in detail at the politics of science and technology. That contemporary societies are constituted as knowledge societies is, of course, an important part of the reason. It follows that important aspects of political behaviour and action cluster around the ways in which knowledge is generated, disputed, and used to underwrite collective decisions"[15].

Habermas states that "a portion of the public sphere comes into being in every conversation in which private individuals assemble to form a public body. Citizens behave as a public body when they confer in an unrestricted fashion –that is with the guarantee of freedom of assembly and association and the freedom to express and publish their opinions- about matters of general interest"[16].

Based on these theoretical analyses, the deployment of biometric systems requires not only government debates on the introduction and deployment of biometric technology, but also citizens, academics and activist groups expressing their opinion, in open discussion about biometric information, including risks and advantages, but in plain language without technical terms[17].

The idea of participation as public debate has proliferated in recent years. Today, there is a broader wave of interest in situations where citizens communicate with each other about matters of public concerns through the Information and Communication Technology (ICT). But, at the same time there are increasing

[15] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4, p. 6.
[16] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4, p.49.
[17] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.

scientific complexity topics, such as genetics or biometrics, along with a lack of social consensus about how these types of technology should be managed.

"Open public debate" is aimed at producing reasonable, well-informed opinion in which citizens are willing to revise preferences and new information. Therefore, open public debate should be understood as a procedure to improve decision making. Habermas and Jasanoff have theorized and studied how "open public debate" have emerged and how they play an important role in generating ideas and information that can improve knowledge, understanding and enhance decisions[18]. They have also examined the circumstances where "open public debate" becomes distorted through manipulation, coercion and misinformation. Habermas focuses on the social and cultural functions that are served by the "open public debate". These deliberative spaces, for him, are considered to be an ideal kind of social environment where citizens can discuss and debate common concerns, access a wide range of information, and reflect and revise their understanding of issues[19].

The aim of "open public debate" is completely different from technocracy movement. The technocracy movement was marked by a high degree of optimism about scientific expertise and the merits of technology that would eventually lead to improvements in efficiency, environmental quality and quality of life[20]. According to Jasanoff, this highly scientific approach failed when they left little room for public participation and discussion, since such activities were viewed as unnecessary roadblocks to technological progress[21]. However, in recent years, for her, scholars have again pushed our understanding of the value of local knowledge and citizen science. They have helped us to critically examine scientific and technical information, and to value a broader array of knowledge that can assist in decision making[22]. Today, several democratic systems have positioned public participation

[18] Idem
[19] Habermas, Jürgen, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society (Studies in Contemporary German Social Thought)*, (Massachusetts Institute of Technology, 1991)
[20] Fischer, F. Citizens, experts, and the environment: The politics of local knowledge, (Duke University Press, 2000)
[21] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4
[22] Idem

activities at the centre of their decision-making processes; creating new models of relationship between State and citizens.

Following this theory[23], several models of the relationship between State and public information can be found. For example, an open data or freedom of public information model, recognizes a citizen´s right to access information by a formal request to public authority or to have information released to the public by the government. These models represent different conceptions regarding the State's obligations of transparency and accountability to inform its citizens. But, both models of open data and of freedom of public information recognise the capacity of governments to be closer to citizen's needs in relation to the deployment of biometric technology[24]. In addition, these models can be interpreted as transparency and accountability as a control mechanism.

For Villanueva "transparency" is "the obligation of government authorities to perform, as a general rule, their actions publicly, as a mechanism to control power and promote democratic legitimacy of public institutions"[25]. Transparency and accountability for Villanueva would consist in biometric systems being subject to public knowledge and assessment by citizens. Particularly, the following information would be available:

a) Information regarding the public management of biometric databases;
b) Criteria on which the decisions are made to implement biometric technology and TBIF; and,
d) Reports on the behavior of public officers using or deploying biometric systems and TBIF[26].

There are two related criticisms, on one hand, that public will not maintain an active interest without hope of influencing a decision or changing a situation. On the other,

[23] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[24] Idem.
[25] Villanueva, Ernesto, *Derecho a la información*, (Porrúa-Cámara de Diputados-Universidad de Guadalajara, 2006) pp. 69-72.
[26] Idem.

that public will not understand these issues. These criticisms have been the primarily concerns from the democratic theory approach. In fact, the analysis of the effects of public involvement on decisions remains somewhat unsolved. Nevertheless, from the modern technology theory approach the “open public debate” considers that the optimal solution is derived from extensive discussion and debate that favours some form of consensus decision making. Where optimal decisions are therefore understood in the context of balancing competing interests, where all players (citizens, academics and activist groups) are engaged in the process, but overall have a fair chance of influencing the final outcome[27].

Modern technology theory approach is more concerned about the processes of representation, participation, involvement and inclusion[28]. For example, in a participatory process of biometric systems deployment decision making, the questions to ask shall be, “Do the participants represent all significant sectors of the community?”. In addition, Jasanoff have address issues of local versus nonlocal participation, lay versus expert participation, and diffuse versus concentrated interests[29].

This chapter highlights the necessity for informed public discussion accompanying the rapid developments in biometric systems. This is a central theme of this thesis. However, it is possible to pose a question regarding if citizens will understand biometric systems issues. Jasanoff explains that internal exclusion may rise even when individuals and groups are nominally included. Such situations occur when opportunities for discussion are limited to certain key spokespersons and specific (technical) kinds of arguments[30]. Jasanoff argues for different modes of practices that allows a linkage among knowledge, technology and power within contemporary industrial democracies[31].

[27] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, “Sfera pubblica (Una voce di enciclopedia)”, above n 4.
[28] Idem
[29] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4
[30] Idem
[31] Idem

Further multidisciplinary research regarding the role of this type of technology is relevant to other legal fields that are beyond of this thesis. More public debate, transparency and accountability about the benefits and risks of biometric systems and TBIF should be available to citizens.

2.3. The Biometric Systems Debate: Tracking History

This section considers a well-established technical literature explaining biometrics, as well as the difference between the terms biometry and biometrics. This examination of the literature provides both an understanding of biometric terminology and how legal implications will be shaped by specific contexts of biometrics.

It is possible to identify two types of literature on biometrics. In the first type, most of the literature explains biometry from the statistical science point of view, as applied in biology. The second type, explains how biometrics has been used as a technique in different scientific fields. However, these two scientific types do not explain the social and legal relationships of biometrics between citizens and governments.

A multidisciplinary approach can be used to identify another type of literature. This approach can be grouped into an historical background to biometric systems[32]. Here, it is possible to trace when and how biometric systems have been implemented. This literature considers and explains the relationship between citizens and governments by using biometric systems in law enforcement, such as forensic analyses and criminal anthropology. There has been discussion on the use of biometric systems in public policies for immigration and/or human social policies, examples of which are the cases of Germany during the Nazi period, the United States and northern Europe during the eugenics movement. A significant characteristic of the well-established technical literature is the attempt to articulate biometric knowledge by explaining biologically inspired models for biometric features, technologies, techniques and applications. This literature goes from the biological “concept of evolution” to the social “eugenics movements”. However, these discussions failed to meet the expectations for legal analysis and more open debate identified by Jasanoff and

[32] For further details, see subsection 2.3.2. The Historical Background of Biometric Systems

Habermas, who would argue that this literature fails not only to publicly discuss biometrics, but also fails to involve all sectors of a society[33].

The specialised literature has always directed its attention to: objectives, purposes, characteristics and applications of biometric systems. Nevertheless, it seems that social, ethical or privacy and data protection implications of biometric systems have not created great interest to be included in all technical literature.

2.3.1. *Definition: Biometry or Biometrics?* According to the general literature, Sokal and Rohlf have accredited the term "biometry" to Pearson and Weldon[34], while for Armitage, the term "biometric" was first used by Bernoulli, in 1841[35]. The terms "biometry" and "biometric" derive from the Greek words *bios*, life and *metron*, measure. The Australian Concise Oxford Dictionary defines the noun biometry as "the application of statistical analysis to biological data" and the adjective biometric as "of or pertaining to biometry"[36]. The Dictionary of Genetics defines biometry as "the application of statistics to biological problems"[37]. These terms have been used in different fields, for example biology, medicine and agronomy. It is possible to assume that biometrics measures biodiversity using statistics.

After analysing the literature, three questions are posed: first, which term do researchers use? Second, is there any difference in the meaning of these terms? And finally, is biometrics a science or a technique?

In this field of study, these questions are central and fundamental to any legal discussion. The language and definitions are not consistent and their meanings can

[33] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[34] Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, above n 7, p. 3; Norton, B.J., "The Biometric Defence of Darwinism" (1973) 6(2) *Journal of the History of Biology* 283-316.
[35] "In 1896 Galton had toyed with the word 'phylometry', and that Pearson suggested 'biometry' for 'the science which applies the modern theory of statistics to the study of variation and correlation in living forms". Armitage, Peter, "Biometry and Medical Statistics" (1985) 41 *Biometrics* 823-833.
[36] Moore, Bruce (ed.), *Australian Concise Oxford Dictionary*, (Oxford University Press, 5th ed., 2009).
[37] King, Robert C. And William D., Stansfield, *A Dictionary of Genetics*, (Oxford University Press, 5th ed., 1997), p. 41.

be ambiguous. For example, in 1963, in 1973 and later in 2003, Sokal and Rohlf[38] define "biometry" as the "application of statistical methods to the solution of biological problems. The original meaning of biometry was much narrower and implied a special field related to the study of evolution and natural selection; however, the wider definition is customary now. Biometry is also called biological statistics or simply biostatistics"[39].

Whereas Hopkins states that "[t]he strict definition of biometrics is the science that involves the statistical analysis of biological characteristics"[40]. However, further along in the same article, he refers to the term as:

> "[T]he statistical analysis of biological characteristics. The use of the term 'statistical analysis' itself implies that interpretation of the biometric data is necessary. Biometrics is not therefore an exact science. It needs to take into account different mechanisms for interpretation of data and different environmental conditions when the data was captured"[41].

Hopkins tried to establish biometrics as a science. However, he recognises that biometrics cannot give solutions or answers by itself; a requirement for it to be considered a science.

By contrast, Zhang defines the term biometric as "technology that uses human being's unique physical or behavioural features to identify or verify persons. It relies on 'something that you are' to make personal identification and therefore can inherently differentiate between an authorized person and a fraudulent impostor"[42].

As mentioned above, the definitions set in specialised literature are not consistent and suggest that the terms "biometry" and "biometrics" are employed in two senses

[38] A pupil of Sewell Green Wright, who developed with Ronald A. Fisher and J.B.S. Haldane Theoretical Population Genetics and established a related discipline of quantitative genetics.
[39] These authors use plain language. Sokal, Robert and James, Rohlf *Biometry*, (W.H. Freeman and Company, 3rd ed., 2003), p. 1-2 and Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, above n 7.
[40] Hopkins, Richard, "An introduction to biometrics and large scale civilian identification", above n 7.
[41] Idem.
[42] Zhang, David, *Automated biometrics: technologies and systems,* above n 7, p. 1.

or with two meanings. The first is scientific, represented by Hopkins as measurements or the statistical[43] study of biological phenomena or processes, as well as the physical properties of living beings; the second, represented by Zhang, is the application of a technique that consists of recognizing and/or verifying a person's identity based on physical and behavioural characteristics.

Therefore the main difference between the terms "biometry" and "biometrics" is how authors apply them. However, nowadays the term "biometrics" has been used in the context of automated systems.

From our perspective there are three concepts that create some issues regarding biometrics. These three concepts are: technique, science and technology. Biometrics seen as a technique relates to the production of things; it implies an empirical knowledge of how to collect biometric information, such as samples, patterns or minutiae. While biometrics seen as a science regards exclusively to the generation of new knowledge through research. Biometric technology refers to an advance degree of knowledge; is the "know how" to do automated biometric systems based on scientific grounds[44].

Technique, science and technology differ in the various objectives pursued: science seeks to understand nature and society; technique and technology seek to produce goods and provide services[45]. Therefore, this thesis will refer to the term "biometrics" as the technique in charge of identifying, or authenticate the identity of a person based on physical or/and behavioural characteristics. In the following chapters, the thesis will refer to the term "biometric systems" as a specific form of technology used to identify or authenticate people.

[43] The Encyclopedia of Genetics defines "Statistics" as "The scientific discipline concerned with the collection, analysis, and presentation of data. The analysis of such data depends on the application of probability theory. Statistical inference involves the selection of one conclusion from a number of alternatives according to the result of a calculation based on observations". Reeve, Eric C.R. (ed.), "Statistics", *Encyclopaedia of Genetics*, (Fitzroy Dearborn Publishers, 2001), p. 324.
[44] Tamayo y Tamayo, Mario, *El Proceso de la Investigación Científica*, (LIMUSA, 2011)
[45] Idem

2.3.2. *The Historical Background of Biometric Systems*. For a multidisciplinary approach, this chapter identifies biometric systems through related historical events. In fact, some historical events have helped to develop biometrics, and assist in understanding the terms "biometry" and "biometrics" and how they have been applied. Human anatomy has long been studied using biometrics as a technique and one of the most important examples was the eugenics movement.

- *Biology represents the background of biometrics and genetics*

The first historical biometric event was recorded in 1858. Herschel captured hand images for identification purposes. He stamped a handprint on the back of each worker's contract to distinguish his employees from others who might claim to be employees when payday arrived.[46] In those years, the study of population structure was widespread because of the concept of "evolution interest". In 1859, Darwin published *On the Origin of Species*[47].

In 1865, Mendel discovered what today we call Mendel's Laws of Inheritance[48]. Two years later, Darwin published *Variation in Animals and Plants under Domestication*[49].

By 1869, Wilson had measured the heads of 464 criminals, "finding their average size less than that of the ordinary population, and coming to the conclusion that 'the cranial deficiency is associated with real physical deterioration'"[50]. Twenty years after Darwin published *On the Origin of Species*, the idea of evolution gained currency and as a result Galton[51] published *Natural Inheritance*[52].

[46] Herschel, William J. "The Origin of Finger-Printing" in Gavan Tredoux (ed) (*Oxford University Press*, 2004) http://galton.org/fingerprints/books/herschel/herschel-1916-origins-1up.pdf (18/12/2012)
[47] Darwin, Charles, *On the Origin of Species,* (Murray, 1859).
[48] Weldon, W.F.R., "Mendel's Laws of Alternative Inheritance in Peas" (1902) 2(1) *Biometrika* 228-254.
[49] Darwin, Charles, *The Variation in Animals and Plants under Domestication* (Murray,1868)
[50] Havelock, Ellis, *The Criminal*, (Scribner & Welford, 1890). http://archive.org/details/criminal00elli (09/12/2012)
[51] "Galton's major contribution to biology is his application of statistical methodology to the analysis of biological variation, such as the analysis of variability and his study of regression and correlation in biological measurements". Sokal, Robert and James, Rohlf, *Biometry*, above n 7, p. 4.
[52] Galton, Francis, *Natural inheritance* (MacMillan, 1889)

- *Forensic analysis and biometrics have the same roots*

The first forensic studies were developed during 1880s. At that time, Bertillon[53] developed the Bertillonage system, an alternative method of fingerprints which consisted of measuring body parts to identify criminals[54]. Bertillon also developed "metric photography" in which identification photographs and visual images of crime scenes are standardized. Currently, the rules of *Bertillon's Metric Photography* are still in force in forensics[55].

Herschel sent his records to Galton and in 1892, he was able to confirm that fingerprints do not change over the course of an individual's lifetime. He presented a basic classification system using prints from all fingers, which proved that no two fingerprints are identical[56].

In 1896, Vucetich[57] worked and perfected the Galteneano system. His fingerprints system was known as Vucetich's system[58]. However, almost at the same time, criminal investigation in British India developed by Edward Henry overthrew Bertillonage and expanded Galton's fingerprints classification system[59]. The Henry classification system allows for the logical categorization of ten-print fingerprint records into primary groupings based on fingerprint pattern types[60]. Consequently, fingerprints can be considered as oldest biometric identification system.

---

[53] Officer at the French Police in 1883. "Bertillon system". *Encyclopædia Britannica. Encyclopædia Britannica Online.* Encyclopædia (Britannica Inc., 2013) http://www.britannica.com/EBchecked/topic/62832/Bertillon-system (9/12/2012)

[54] Idem

[55] Idem

[56] See the website of "Sir Francis Galton", Galton.org http://galton.org/ (14/01/2013)

[57] A Croatian immigrant to Argentina.

[58] Locard, Edmond, *Manual de Técnica Policiaca*, (Editorial Maxtor, 1935), p. 104.

[59] Galteano system defined some of the points or characteristics from which fingerprints can be identified.These "Galton Points", also known as "minutiae" are the foundation for the fingerprint identification, which has expanded and transitioned over the past two centuries. Galton, Francis, Fingerprint Directories (MacMillan, 1895) see the website of "Sir Francis Galton", Galton.org http://galton.org/ (14/01/2013)

[60] Beavan, C., *Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science,* (Hyperion, 2001).

Biological variation studies were continued by Pearson and Weldon applying statistical methodology to the analysis of biological variation[61]. It is important to highlight that at that time, biology was not regarded a quantifiable science[62].

- *Biometrics shares the same background of genetics and eugenics*

The first studies of genetics started in 1900s. In 1905, Bateson coined the word "genetics"[63] and four years later, in 1909, Wilhelm Johannsen and Nilsson–Ehle rediscovered Mendel's Law of Inheritance, which implies that genetic methods and forensic analysis have the same roots as biometry[64].

Between 1910 and 1940, the dominant figure in biometry was Major Greenwood. He was a critic of the eugenics movement because he believed there was a fundamental conflict between the demands of medical ethics and social conscience, and a rigorous adherence to eugenic principles[65]. In these years, eugenic science[66] was accepted and institutionalized in northern Europe and the United States of America[67]. In Europe, Lombroso and his pupils Ferri and Garofalo, among others, developed the theory of criminal anthropology[68]. Meanwhile in the United States, Daveport published a book entitled *Heredity in Relation to Eugenics*, in which he

[61] "The genetical problem of continuous variation remained therefore a challenge to geneticist; the more so as biometrically Galton and Pearson had clearly shown such variation to be at least in part heredity, even although they had failed to discover the mode of transmission". Mather, Kenneth and Jinks, John L., *Biometrical Genetics. The study of continuous variation*, (Cornell University Press, 1971), p. 2.
[62] see the website of "Sir Francis Galton", Galton.org http://galton.org/ (14/01/2013).
[63] "'Genetics' is a term covering a wide set of theories, practices, and technologies, only some of which overlap with the practices and technologies of biometrics". Van Der Ploeg, Irma, "Genetics, biometrics and the informatization of the body", above n 5.
[64] Hartwell, Leland *et.al.*, *Genetics from Genes to Genomes*, 3rd ed, (McGraw Hill, 3rd ed, 2008), p. 1.
[65] Armitage, Peter, "Biometry and Medical Statistics", above n 35, p. 824; Pearson, E.S. "Studies in the history of probability and statistics. XIV Some incidents in the early history of biometry and statistics, 1890-94" (1965) 52 *Biometrika* 3-18.
[66] Eugenics the science of improving the population by controlled breeding for desirable inherited characteristics. *"In the reasoning of eugenicists, lower income groups were not poor because they had inadequate education and economic opportunities but because their moral and educational capacities, rooted in their biology, were inadequate".* Kevles, Daniel J. And Hood, Leroy (eds), *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, (Harvard University Press, 1993), p. 9.
[67] Idem.
[68] Havelock, Ellis, *The Criminal*, above n 50.

noted that single genes did not seem to determine important mental and behavioural characteristics[69].

Briefly, the development human social problems, such as poverty, insanity, and criminality were associated as a result of hereditary traits and defects. Human genotypes were difficult to measure and have often been treated as unobservable attributes. An example of this arose during the Nazi period:

> "Eugenic research in Germany before the Nazi period was similar to that in the United States and Britain, and much of it remained similar after Hitler came to power. The Institute of Anthropology, Human Heredity, and Eugenics, for example continued to press investigations into subjects such as the genetics of diabetes, tuberculosis, and brain disease: the heritability of criminality: the effects of race crossing (with no particular emphasis on Jews or Aryans)"[70].

During the Nazi period, the idea that all human weaknesses were the result of poor heredity took root. Also, in the United States, immigration was seen as detrimental to 'American' heredity stock[71]. In the Nazi period class and racial prejudice were prevalent and widespread[72].

> "During the Hitler years, however, Nazi bureaucrats provided eugenic research institutions with handsome support and their research programs were expanded to complement the goals of the Third Reich. They exploited ongoing investigations into the inheritance of disease, intelligence, behaviour, and race to advise the government on its biological policies"[73].

---

[69] Kevles, Daniel J. And Hood, Leroy (eds), *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, above n 66, p. 7.
[70] Ibidem, p. 8.
[71] Ibidem, p. 7.
[72] Bresler, Jack, B. (ed.), *Genetics and Society*, (Addison-Wesley Publishing Company, 1973), p. 5 and Kevles, Daniel J. And Hood, Leroy (eds.), *The Code of Codes, Scientific and Social Issues in the Human Genome Project*, above n 66, p. 7-12.
[73] Kevles, Daniel J. And Hood, Leroy (ed.), *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, above n 66, p. 8.

In 1918, that the two theories, Darwin's and Mendel's, were fused by Fisher in *The Correlation between Relatives on the Supposition of Mendelian Inheritance*[74]*.* After that, Fisher and other colleagues as Haldane, Hogben, Huxley and Muller hold that eugenics must be free of racial and class bias, and must also be consistent with what was known about the laws of heredity[75].

> "The new students of human heredity preferred to search for well defined, sharply segregating traits as immune as possible both to uncertainty in identification and to environmental influence"[76].

After 1930, the eugenics movement declined and new studies suggested that human heredity was much more complex than formerly thought[77].

> "[W]elcomed with particular enthusiasm the rapidly increasing knowledge of the human blood groups. The blood groups displayed patterns of inheritance that seemed to conform to Mendel's laws"[78].

In summary, in the late 19th century and the early 20th century, the terms "biometry" and "biometric" were associated with the study of the inheritance of continuous characteristics. These terms were not usually used in a more general sense[79]. In the 1930s, these terms almost disappeared forgotten. However, in 1946, the statistical community promoted the use of the term "biometric" when organising the first International Biometric Conference[80].

> "Biometry first emerged as a speciality within the discipline of biology. Its definition as a separate speciality was largely dependent on its claim that

[74] Mather, Kenneth and Jinks, John L., "*Biometrical Genetics. The study of continuous variation"*, above n 61, p. 3.
[75] Kevles, Daniel J. And Hood, Leroy (eds.), *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, above n 66, pp. 11-12.
[76] Ibidem, p. 12.
[77] Idem.
[78] Idem.
[79] Ibidem, p. 824; Pearson, E.S. "Studies in the history of probability and statistics. XIV Some incidents in the early history of biometry and statistics, 1890-94", above n 65.
[80] Armitage, Peter, "Biometry and Medical Statistics", above n 35, p. 826.

statistical analysis of organic populations would lead to the elucidation of evolutionary processes"[81].

Currently, the term "biometrics" is used for the automated technique for identification and authentication in systems. The use of this type of technology has been intensified and diversified into different fields, particularly for security purposes.

2.3.3. *Biometrics and Popular Culture*. Interestingly, developments in biometric technologies can be traced to ideas from science fiction literature and, later produced in films and television programs. The following table shows some film and television examples of now operational biometric systems.

Figure 2. Science Fiction Literature Associated with Biometrics

Movies and TV shows	Biometric Systems	Implemented by Government	Commercial Product
The Andromeda Strain (1971)	Palmprint	1990 Olympic Games (Atlanta)	1980
Blade Runner (1982)	Iris recognition	1986 used for first time	1995
Tomorrow Never Dies (1997)	Facial recognition	2001 Super Bowl (Florida)	--
Mission Impossible (1966-1973)	Voice recognition	1975 first prototype	1980

Source: Information obtained from Zhang, David, *Automated biometrics: technologies and systems*, (Kluwer Academic Publishers, 2000); Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Boulgouris, Nikolaos V., *et. al., Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al., Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003); Bolle, Ruud M., *et. al., Guide to Biometrics*, (Springer, 2003)

"The Andromeda Strain" (1971), directed by Robert Wise and based on the novel of the same name by Michael Crichton, first showed the biometric system on hand geometry, which also triggered the possibility of performing biometric fingerprints and palmprints. These systems were used for the first time in 1974 by the United States government, but were not fully implemented until the Atlanta Olympic Games in 1990[82].

[81] Farral, Lyndsay A., "Controversy and Conflict in Science: a Case Study –The English Biometric School and Mendel's Laws" (1975) 5 *Social Studies of Science* 269-301.

[82] Zhang, David, *Automated biometrics: technologies and systems,* above n 7; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 7; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 7; Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, above n 7; Bolle, Ruud M., *et. al., Guide to Biometrics*, above n 7.

The second example on the table is "Blade Runner" (1982), directed by Ridley Scott and based partly on Philip K. Dick's novel "Do Androids Dream of Electric Sheep?" (1968). The film shows the iris biometric system for verification, first used commercially in 1986 and which went on sale in 1995[83].

"Tomorrow Never Dies" (1997), the eighteenth film in the James Bond series, shows the face recognition biometric system. The U.S. government implemented it in 2001 during the XXXV Super Bowl (Florida). On that occasion, the police in Tampa Bay, Florida, used the facial recognition biometric system to identify criminals[84].

Finally, the table shows the hit U.S. television series "Mission Impossible" (1966-1973) and shows the voice biometric system for recognition, the prototype of which was developed in 1975 and marketed in 1980[85].

Biometric systems are the result of the functionality and convenience of technologies in operation. Automated biometric technologies have only become available over recent decades and have lately been receiving the attention of popular media. This automated biometric system makes it possible to collect, store, process and exchange massive volumes of biometric data.

2.3.4. *Biometrics is not an Independent Science*. Based on its current use, scientific literature demonstrates that biometrics is not an independent science. As mentioned above, biometrics is a statistical method of acquiring data, and uses observation and experimentation to describe natural phenomena. It has failed to explain the natural phenomena in itself. Biometry can be defined as the study of statistical methods to biological characteristics and the application of technological biology for uniquely identifying or verifying humans based on physical and/or behavioural characteristics.

[83] Idem.
[84] Idem.
[85] Idem.

In summary, biometrics has been studied since 1880s and it has been introduce indirectly in immigration policy in many countries and directly in enforcement law. These techniques have had consequences in both immigration and criminal investigations, which are the focus of this thesis.

2.4. Biometric Systems: Privacy Review

Biometric systems present a legal challenge to privacy, as do many other technologies. In this respect, it is important to explain the historical background to privacy and to identify how privacy and data protection have become recognised as human rights before identifying how privacy has been studied, within the biometric systems literature.

Privacy is an historic reality that has been constructed differently within different societies[86]. According to some authors, the concept of privacy appears with the arrival of Christianity[87]; however, human beings had already enjoyed privacy[88].

In the Middle Age, the concept of privacy was limited in the sense that its regulation at that time did not favour any distinction between private life and public life. "The consciousness of the Western man is based on the idea of being as a purpose in itself, like an autonomous centre of personal life"[89]. It was not until the 18th century that an attempt was made to define "public life and what did not have that character"[90]. Indeed, it was said that "while man made himself in public, he performed his nature in the private realm, mostly experiences within the family nucleus"[91]. It should, be noted, however, that the *Declaration of the Rights of Man*

[86] Privacy is a historic reality because at the beginning of time not all individuals were able to enjoy the right to be alone. In fact it was not seen as a right; rather it was a privilege where a few individuals such as the kings or priests have that "privilege". Later, for example around 1452 in places like the New Spain, the indigenous people were converted to the Christianism and they were forced to pray and stay "alone" with "God". So it is possible to conclude that they were enjoying a moment to be alone. Aries, Phillippe and Duby, Georges, *Historia de la Vida Privada*, (Taurus, 1989) vol 5, p. 189.
[87] Idem; Fariñas Matoni, Luis María, *El Derecho a la Intimidad*, (Trivium, 1983), pp. 315-352.
[88] Fariñas Matoni, Luis María, *El Derecho a la Intimidad*, above n 87.
[89] Pérez Luño, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución,* (Tecnos, 2003), pp. 321-322.
[90] Aries, Phillippe and Duby, Georges, *Historia de la Vida Privada,* above n 86.
[91] Idem.

and of the Citizen, as well as other similar instruments written in the 18th century, did not contain any mention whatsoever of the right of privacy or data protection.

With the birth of Christian thinking in the Middle Ages, the pursuit of intangible goods began to deepen: intangible goods belong to the person who contributes to the progressive development of personal relations. Based on the Christian idea, privacy was considered a basic good belonging to the person, that is, it would become a supreme and sacred value for individual existence[92]. The modern idea of human rights comes from the contrast between nature and culture, recognising that if person´s feelings were hurt or the person humiliated, this would constitute a restriction of their natural rights[93].

Some examples of privacy, prior to the early modern period, are reading of the Bible together as a family, inner dialogue with God, self-seclusion, writing personal journals, and so on. These actions may be deemed internal acts because the individual claims for a space and inner life, an "internal realm", from a religious context. In other words, a demand was denoted in numerous new attitudes and other customs that were not common until that moment. So, the rules of good upbringing and courtesy codes would emerge with the acknowledgement of privacy, in which the need to preserve a space around the body was depicted as an area far from the sight and contact of strangers[94].

In the Modern Age[95], the right to privacy became one of the most important desires of each individual. The ideal was a space free from any interference where the person might enjoy an individual sphere and avoid all kind of intrusions[96].

---

[92] Saint Augustine, in his work *Confessions*, explores privacy systematically and in detail. He says that "a man's inner self transforms into a point of reference in order to reach God, since He is the only One with inner access". San Agustín *Confesiones (*Eugène Portalié trans, Prana, 2006).

[93] Aries, Phillippe and Duby, Georges, *Historia de la Vida Privada,* above n 86.

[94] Martínez Pisón, José, "Vida Privada: Implicaciones y Perversiones", (1997) XIV *Anuario de Filosofía del Derecho* 720-723.

[95] The Early Modern period –from the natural law of the 17th century to the revolutionary declarations of rights– creates a fracture of that era with that of the Middle Ages, which is why the former constituted itself as the Era of Individual Rights and the progressive improvement of their protection because it marked the fall of medieval culture, as well as of the feudal and state organization of government and society. Fioravanti, Mauricio, *Los Derechos Fundamentales: Apuntes de Historia de las Constituciones,* (Trotta, 2003), pp. 35-36.

[96] Martínez Pisón, José, "Vida Privada: Implicaciones y Perversiones", above n 94, pp. 702-713.

Therefore, most of the scholars agree in stating that "the acknowledgement of the right of privacy emerges from liberal systems and consists of an aspiration to have access to what formerly used to be a privilege of only a few. Thus, the idea of privacy was thought of in such way for it to be enjoyed by a select "bourgeois" group, without implying a concern in making it available to the poorest groups of the population. Hence, it could not be considered a universal right"[97].

These first formulations of the concept were proposed by Locke[98]. He started from the so-called "negative freedom" and thought that every human being should own a minimal sphere of recognized personal freedom that must on no account be violated by any other person. It would be an individual's right to react before pressures and external influences, as well as having the freedom to act as that person deems appropriate, according to the regulations that rule over and organize the society in which that individual participates[99].

According to Kant, this right revolves around the orbit of the internal realm; that is, a person's space must be kept free from State interference, as well as separate from community social relations[100]. Like other human rights, the right to privacy has maintained its historicity and positiveness, establishing itself in the modern era[101].

[97] As an example, it is more than enough to consider the material conditions of the life in which the Industrial Revolution took place since workers were excluded from having any private sphere. Pérez Luño, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución,* above n 89, pp. 321-322.

[98] Freedom finds its foundation in three aspects: 1. Autonomy, self-control capacity, 2. Possession, or property that can be demanded from other individuals and before established powers; and, 3. A life plan, an element that organizes an individual's life. Under this concept of freedom, Locke proposes an aspect of freedom called privacy, which is part of the conduct of a rational individual (one who has overcome wild freedom). Locke, John *Second Treatise of Civil Government* http://oregonstate.edu/instruct/phl302/texts/locke/locke2/locke2nd-a.html (18/12/2012) and *A Letter Concerning Toleration and Other Writings* http://files.libertyfund.org/files/2375/Locke_1560_EBk_v6.0.pdf (18/12/2012).

[99] Negative freedom has historically been understood as the ability to act, without obstacles or obligations, within a clearly limited and autonomous sphere, mostly in regards to political power. Fioravanti, Mauricio, *Los Derechos Fundamentales: Apuntes de Historia de las Constituciones,* above n 95, pp. 35-36.

[100] Pérez Luño, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución,* above n 89, p. *322.*

[101] Ruiz Miguel, Carlos, *La Configuración Constitucional del Derecho a la Intimidad,* (Tecno, 1995); Rebollo Delgado, Lucrecia, *El Derecho Fundamental a la Intimidad,* (Dykinson, 2005).

The specialised literature on privacy generally adopts three approaches in modelling the concept of "privacy": privacy as information control (self-determination)[102], privacy as non-interference[103] and privacy as a condition of limited accessibility[104].

The core provisions on the modern conception of the right to privacy can be found in the main human rights treaties, the *United Nations Universal Declaration of Human Rights* (Article 12) and the *International Covenant on Civil and Political Rights* (Article 17). For the purposes of this thesis, other important regional human rights instruments are the *European Convention on Human Rights* (Article 8) and the *American Convention on Human Rights* (known as the Pact of San Jose, Costa Rica) (Article 11).

It is important to note that in 1990, the United Nations General Assembly issued specific *Guidelines concerning Computerized Personal Data Files*[105]. However, the 1980 Organisation for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* commanded the greatest influence on the international community.

Bygrave acknowledges that in 2000, when the *Charter of Fundamental Rights of the European Union* (CFRUE) was enacted, the right of data protection was incorporated

[102] Perhaps the most representative scholar in this field is Alan Westin who discussed "the functions of privacy for individuals and organizations in democratic societies, and the nature of invasion of privacy and surveillance". (when, how and to what volume information about them is disclosure to others) Westin, Alan, "Science, Privacy and Freedom: Issues and Proposals for the 1970's" (1966) 66(7) *Columbia Law Review* 1003-1050.

[103] Developed by Samuel D. Warren and Louis D. Brandeis, who argued that "now the rights to life has come to mean the right to enjoy life, -the right to be let alone: the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession- intangible, as well as tangible". Warren, Samuel D and Brandeis, Louis D. "The Right to Privacy" (1980) IV(5) *Harvard Law Review* 1-23, http://www.estig.ipbeja.pt/~ac_direito/privacy.pdf (18/12/2012)

[104] For Ruth Gavison, the concept of privacy consists of three elements: "'secrecy' -the extent to which we are known to others; 'solitude' -the extent to which others have physical access to us; and 'anonymity' -the extent to which we are the subject of others' attention. These three elements are distinct and independent, but interrelated". Gavison, Ruth "Privacy and the Limits of Law" (1980) 89(3) *The Yale Law Journal Company* 421-471.

[105] Rule, James B and Greenleaf, Graham, *Global Privacy Protection*, (Edward Elgar Publishing, 2008), p. 29.

internationally in a human right instrument[106]. Before that, data protection as international human right had been derived indirectly in the protection of the right of privacy[107]. Moreover, Bygrave highlights that Article 8 of the CFRUE does not define the right of data protection, but instead states a systematic categorization of the principles of data protection and supervision by an independent data protection authority[108]. The principles expressly mentioned are fair and lawful processing, specified purposes, consent, access to data and rectification.

2.4.1. *The Legal Impact on Privacy and Data Protection*. Privacy is the right of an individual to remain free from intrusions, to be autonomous and to control access to his/her personal information[109]. This section will argue that biometric technology presents an inherent challenge to privacy and data protection rights. International and national privacy and data protection regimes are discussed in greater detail in further chapter[110].

It is important to highlight that in the 1970s, studies on the automatic processing of personal data started as a reaction to the potential and capability of computer

[106] The Charter is a declaration signed by the presidents of the European Parliament, the European Council and the European Commission on December 7, 2000. *Charter of Fundamental Rights of the European Union* [2010] OJ C 83/02.
[107] Bygrave, Lee, "The Place of Privacy in Data Protection Law", above n 5.
[108] Idem.
[109] *Universal Declaration of Human Rights, adopted by G/A/RES 217A (III) on 10 December 1948*, Article 12; *American Declaration on the Rights and Duties of Man, adopted by the Ninth International Conference of American States, April 1948*, Article V. and *American Convention on Human Rights, opened for signature 22 November 1969 (entered into force 18 July 1978)* Article 11.
[110] For further details, see Chapter 7. Transborder Biometric on Privacy and Data Protection: National Solutions

systems to collect, store and process personal information[111] until 2000 when data protection was recognised as a human right in the CFREU[112].

Under this theoretical framework it is possible to identify the main impact on privacy and civil liberties: intrusiveness, the loss of privacy, the disclosure and possible misuse of personal information. However, the advancement of technology exposes the impact of uncertainty in areas dealing with securing personal information transmitted through electronic identification systems (eID), the purpose and misuse of information in electronic storage capacity and individuals' knowledge or consent in electronic collection of information capacity. In addition to this, there are concerns about identity theft.

> "A man without privacy is a man without dignity: the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars"[113].

Intrusiveness, the loss of privacy and the disclosure of personal information are three examples of the inherent challenge of biometric technology because:

[111] In 1970, the first data protection law in the world was enacted in the Land of Hesse in Germany; then, Sweden in 1973, the United States in 1974, Germany in 1977, France and Norway in 1978 and so on. It is interesting to show that this "data protection movement" started in Europe in the 1970s, while in Latin American countries, the movement started in the 1990s by regulating both sectors – public and private- databases. In fact, for example, Brazil in 1997 and Chile in 1999 became the first Latin American countries to enact a data protection law. However, Argentina and Uruguay are the only Latin American countries to receive certification from the European Union on "adequate protection of personal data". Argentina received it in 2003 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003D0490:ES:HTML (18/12/2012) whereas Uruguay received it in 2012 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:227:0011:01:EN:HTML (18/12/2012)

[112] The most pioneering aspect is the recognition of a right to protection of data, of which there are three: *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* OECD (23 September 1980), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1985), as amended by *The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, opened for signature 15 June 1995, (entered into force after acceptation by all Parties), as amended by the *Protocol to Convention ETS No. 108,* opened for signature 8 November 2001, ETS No. 181 (entered into force after acceptation by all Parties) and the *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31.

[113] Cowen, Zelman "The Private Man" (1969) *The Boyer Lectures*, Australian Broadcasting Commission 9-10.

- First, biometric characteristics are physical and behavioural measurements in origin and biometric technology might acquire additional personal information from scanned biometric features[114]. That is, the case of features found in the eyes (retina and iris) could reveal blood pressure disorders and diseases like glaucoma. This derived information could be used as a basis for discrimination. In addition, biometric characteristics are not secret because one of the conditions is their universality[115]. It is possible to obtain an individual's pattern without his or her knowledge or consent, such as face data with CCTV and fingerprints with sensors.

- Second, biometric technology –such as fingerprints and facial recognition systems- allows for the possibility of obtaining identifications that are unwanted due to safety reasons. Individuals in the witness protection program could be identified based on their fingerprints or facial recognition[116]. In addition, minors could be identified because biometric technology does not make any distinctions regarding age.

- Third, biometric technology combined or used with Radio Frequency Identification (RFID), any Global Positioning System (GPS) or any Automatic Identification and Data Capture (AIDC) technology empowers not only the identification or authentication of people, but it also increases the collection of data without their knowledge or consent. Software platforms or applications available for both public and private sectors could link biometric information with more personal information about individuals enrolled in widely different databases or electronic systems. An example of this fusion of technologies is ELISE, a platform that combines multiple biometrics and biographic data in a single search developed by the company WCC Smart Search and Match[117].

---

[114] Prabhakar, Salil *et. al.,* "Biometric Recognition: Security and Privacy Concerns", (2003) 41 *IEEE Security & Privacy* http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1193209&tag=1 (18/12/2012).

[115] As discussed further in this chapter, every person should have the characteristic because biometric characteristics are not secret. For further details, see Section 2.5. Biometric Characteristics: Typology

[116] Prabhakar, Salil *et. al*., "Biometric Recognition: Security and Privacy Concerns*",* above n 114.

[117] This company is identified in Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships. For further information about ELISE, see WCC Smart Search & Match

Today, the intensification and diversification of biometric technology poses an increasing risk on privacy and civil liberties. Through interactive platforms it is possible to deliver personal services or online interactions like electronic commerce, electronic government, electronic health and electronic education, among other electronic activities. While personal data is collected, stored, analysed and exchanged in most cases to grant access to multiple electronic identification systems (eID) both on and off the Internet[118], in other cases, it is done for law enforcement, commercial, social or marketing purposes or simply for convenience.

These interactive platforms have set the role of a strong electronic identity[119]. Furthermore, the advancement of storage capacity of personal information and the facilitation of information flow creates legal concerns regarding the purpose and misuse of information (subsequent use of personal information).

The biometric industry has been centring its attention on highly secure access-control applications, in which the primary objective is to deter impostors and avoid threats against biometric systems.

Most biometric information is stored on electronic servers, networks or private clouds and a common threat is cyber-crime. The threat of any information system range from relatively harmless intrusions like viruses, worms, Trojan horses to the

official website http://www.wcc-group.com/page.aspx?menu=products_001&page=products_software (18/12/2012)

[118] For example, under the United Kingdom *Identity Cards Act,* information that may be recorded is prescribed by Schedule 1. Schedule 1 information that may be recorded are personal information, identifying information, residential status, personal reference numbers, record history, registration and ID card history, validation information, security information and records of provision of information. Personal information that may be recorded: an individual's full name, other names by which he/she is or has been known, date and place of birth, gender, the address of his/her principal place of residence in the UK, the address of every other place in the UK or elsewhere where he/she has a place of residence. Identifying information that may be recorded: a photograph of his or head and shoulders (showing the features of the face), signature, fingerprints and other biometric information about him or her; the rest of the information is related to citizenship and residential status, including residential address, nationality, identity card number, passport number, work permit number, driver's licence number and administrative information such as security and verification details. *Identity Cards Act 2006* (UK) schedule 1.

[119] Electronic Identity documents –national ID cards, ePassports, driving licenses and display credit cards, among others- hold one or two biometric data, such as a photograph and/or fingerprints. It may incorporate multiple security features to prevent counterfeiters, as well as RFID or AIDC technology.

disruption of critical information systems like fraud or identity theft[120]. Thus, privacy concerns are about uncertainty in securing personal information, the disclosure of information and identity theft.

The use of biometric technology certainly challenges privacy and civil liberties[121]. Thus, it is not only important to have an adequate privacy and data protection legal framework that covers biometric information[122], but also to have citizens involved and participating in an informed public policy debate. The deployment of biometric systems should be accompanied by transparency and accountability, as a public interest control mechanism[123]. In addition, it is important that the biometric industry does not failed to acknowledge the weakness of their products and offer solutions in the form of system architecture, design consultation, installation support and customer training to avoid any negative impact for their clients[124]. Otherwise, not only will it affect the balance of human rights, but it could also raise financial and technical issues for their clients. The deployment of biometric technology transcends national borders. This issue will be discussed in later chapters.

2.5. Biometric Characteristics: Typology

After tracking privacy and data protection rights recognition and reviewing the specialised literature related to biometrics this section centre its attention to biometric typologies. Biometric typologies are categorized in terms of physical or behavioural characteristics and more detailed information on biometrics typology is included in Appendix B.

[120] Cybercrime is defined as "unauthorised acts leading to the interruption, modification or fabrication of information flows*".* Stallings, William, *Data and Computer Communications*, (Prentice Hall, Upper Saddle River, 2004), p. 5.
[121] This is one of the main arguments of this thesis. For further details, see section 1.4 Hypothesis
[122] For further details, see Chapter 7. Transborder Biometric on Privacy and Data Protection: National Solutions
[123] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States*, above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di encyclopedia)", above n 4.
[124] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

There is also another classification based on software according to signal types (one dimension or two dimensions) or sensor types (touching or non-touching) used in biometric technologies. However, they will not be discussed in this thesis as they are related to engineering systems.

The general agreement set by the specialised literature considers that the physical and behavioural characteristics chosen for identification purposes should basically satisfy five conditions: 1) Universality, every person should have the characteristic; 2) Uniqueness, there are differences between individuals based on this characteristic; 3) Permanence, the characteristic should not change much with environment or over time; 4) Collectability, the characteristic can be measured; and 5) Acceptability, the public in general should have no objection to having the biometrics collected[125]. The following figure presents the most popular biometrics typology.

Figure 3. Biometric Typology

Biometric Typology	
Physical Characteristics	• Chemical composition of body. • Thermal emissions. • Iris and retina patterns. • Fingerprints. • Palmprints. • Hand geometry. • Face. • Pores of the skin.
Behavioural Characteristics	• Handwritten signature. • Voice. • Keystrokes. • Gait.

Source: Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, (W.H. Freeman and Company, 1973); Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*"* (1999) 13(3) *International Review of Law, Computers & Technology* 337-363; Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000); Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003); Bolle, Ruud M., *et. al.*, *Guide to Biometrics*, (Springer, 2003)

Specialised literature emphasizes that these physical and behavioural characteristics are unique: they cannot be stolen, forgotten, duplicated or shared. However, no single biometric system has clear attributes that will guarantee its ascendancy over

[125] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 7, p. 5; Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*",* above n 7; Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, above n 7, p. 71-130; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 7; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 7.

the others. Each has its strengths and its weaknesses[126]. Given this uniqueness of biometric characteristics the importance of public debate is critical to publicise not only the interaction between citizens and technology, but also the interaction between governments and biometric industry[127].

2.5.1. *The Special Case of DNA (Deoxyribonucleic Acid)* DNA is a very special case in biometric characteristics. Specialised literature is divided; for example Zhang does not consider DNA as a physical characteristic for biometric systems whereas Van der Ploeg does. This thesis however treats and recognises DNA as a physical biometric characteristic[128].

Human beings have several thousands of genes –specific DNA sequences in specific areas of the chromosomes- and each gene represents a specific sequence of amino acids that creates RNA for the formation or coding of specific proteins[129]. Different versions of a gene appear as a pair of alleles at a specific position, and a specific collection of alleles are labelled as a genotype. While over 99 per cent of all genes in humans are identical to the corresponding genes in all other humans, the other one per cent is important because that one per cent is thought to lead to individual differences in both genotypes[130]. Human beings exhibit several thousands of observed behaviours and any well-defined subset of these behaviours is labelled a phenotype[131].

The methods of genetic analysis of behaviours are used to elucidate and improve our understanding of the relationships among particular variations or combinations of genotypes and particular variations or combinations of phenotypes[132]. In 1998, the

[126] Idem.
[127] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships
[128] In his book, Zhang does not includes or mention DNA as a biometric characteristic. Zhang, David D. *Automated Biometrics Technologies and Systems,* above n 7. However, Van Der Ploeg, *Irma, Genetics, biometrics and the informatization of the body*, above n 5.
[129] "The phrase 'methodology in genetic studies of behavioural' is intended to cover any scientific analysis of behavioural phenomena that includes biometric genetic information." McArdle, J.J. and Allison, D.B., "Genetic Studies of Behaviour: Methodology", *International Encyclopaedia of the Social & Behavioural Sciences*, (Elsevier, 2001), pp. 6108-6116.
[130] Idem.
[131] Van Der Ploeg, *Irma, Genetics, biometrics and the informatization of the body*, above n 5.
[132] Idem.

FBI launched the Combined DNA Index System (CODIS) to digitally store, search and retrieve DNA markers for forensic law enforcement purposes[133].

2.6. Biometrics Profiles: How are they Created?

The templates of physical and behavioural characteristics are used in biometric systems. Biometric profiles are created by using templates. This section discusses the content of biometric DNA databases.

Biometric profiles are biological samples[134], which usually contains human genetic information to determine the exclusive sequence or the identity of a person. The information obtained from blood, skin, bone cells or blood plasma can be digitally stored in automated databases[135].

These databases manage different categories of information regarding genetically individualized criminals, evidence found at a crime scene or even genetic information from the victims. Therefore, the data collected in these databases is corresponds to natural or physical characteristics of persons identified or to be identified. Thus, handling this information should be in accordance to regulations for privacy and personal data protection[136]. As this is sensitive information collected, stored and exchange in these biometric databases[137], civil society, industry, special advocates and public official should also be involved in public debates about the introduction, development and operation of these databases[138].

---

[133] Wayman, James*, et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 7; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 7; Bolle, Ruud M., et. al., *Guide to Biometrics*, above n 7.

[134] Any sample of biological material (for example blood, skin and bone cells or blood plasma) in which nucleic acids are present and that contains the characteristic genetic make-up of an individual. *International Declaration on Human Genetic Data*, opened for signature and adopted 16 October 2003, article 2 (IV).

[135] Van Der Ploeg, *Irma, Genetics, biometrics and the informatization of the body*, above n 5.

[136] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

[137] For further details, see section 1.2. The Context of the Study: Deployment of Biometric Systems

[138] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4, p. 4.

2.7. Biometric Systems: How do they Work?

Physical and behavioural characteristics are used as a technique for identification (recognition) and authentication (verification). This technique is known as biometric systems. Biometric systems can be designed to be automated or manual. This section discusses the use, purposes and limits of biometric systems.

Specialised literature recognises that there are other techniques that have been used to identify and verify humans, which include, for example, a variety of types of credentials, passwords or tokens. The main difference between the other methods and biometric characteristics is that the person him/herself is the key[139].

These visible characteristics are unique to each individual and cannot be transferred as discussed in preceding section[140]. Biometric systems have been progressively associated with enhanced security[141] which demands public policy debate regarding the deployment of such biometric systems.

Biometric systems have two objectives (identification or authentication) and are designed based on their objectives. Identifying and verifying are different activities, which is why some biometric systems are more appropriate for recognition (identification) than authentication (verification) and specialised literature acknowledges this[142].

Likewise, it is not possible for everything to be considered a biometric characteristic in itself, for example blood type, weight, height and shadow, among others. In some cases, biometric systems either for identification (recognition) or authentication (verification) require that two or more characteristics be measured. Combined

[139] Routine photographs, radiographs and dental impressions are examples of other methods used to identify.
[140] Uniqueness is the direct result of the individual differences that exist in the development of a body's anatomical structures. For further details, see Appendix B. Biometrics Typology
[141] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges
[142] Wayman, James*, et. al., Biometric Systems Technology Design and Performance Evaluation*, *above n* 7; Boulgouris, Nikolaos V., *et. al*., *Biometrics, Theory, Methods, and Applications*, above n 7; Bolle, Ruud M., et. al., *Guide to Biometrics*, above n 7; Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 7*.*

biometric systems, for instance blood type and DNA, are used because the type of blood by itself does not identify a specific person. Combining two or more biometric technologies yields better performance and reliability, reducing biometric systems' false rejections and false acceptance rates[143].

Bolle explains that biometric systems require processing unique data that is extracted from the sample and a template is created. Physical characteristics are rich enough that a onetime sample may be sufficient for comparing templates. For behavioural characteristics, any given sample may not give any information about a person's identity, but it is the temporal variation of the signal that contains the information[144]. Meanwhile, Zhang highlights that the templates for any two persons should be different, and different samples from the same person should be similar enough[145].

For Zhang, Hopkins and Boulgouris, the two important operations in a biometric system are enrolment and testing because, in cases of enrolment an individual's biometrics in a database, and during the testing phase, an individual's biometric information is detected and compared with that stored in the database[146]. For more detailed information on how biometric systems work, see Appendix C[147]. As stressed in this thesis[148], it is crucial that governments inform to citizens about the creation and management of these biometric databases.

2.8. Purposes and Limits of Biometric Systems

The development of biometric systems depends on the purposes of the identification or verification, which are in themselves different activities. The following figure presents how biometric systems work. Identification or recognition aims at determining who subject is without information given by the individual. Identification

[143] Boulgouris, Nikolaos V., *et. al., Biometrics, Theory, Methods, and Applications*, above n 7, p. 69.
[144] Bolle, Ruud M., *et. al., Guide to Biometrics*, above n 7, p. 4.
[145] Zhang, David D., *Automated Biometrics Technologies and Systems*, above n 7, p. 10.
[146] Idem; Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*",* above n 7; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 7.
[147] For further details, see Appendix C. How Biometric Systems Work
[148] For further details, see section 2.2. Comments on the Articulation of Biometric Knowledge

and recognition mean that characteristics are selected from a database to produce a list of possible or likely matches[149]. Meanwhile, authentication or verification as the name suggests seeks to verify the individual based on information provided by the user. Authentication and verification mean that when a person makes a claim that he or she is a specific person, only that specific person's characteristics are checked to see if they match[150].

Figure 4. Purposes of Biometric Systems

How Biometric Systems Work	
Authentication (verification)	➢ The person being checked enters a password or swipes his/her identification card. ➢ The system captures his/her biometrics feature(s). ➢ The captured data is processed and compared with the one associated with the password or identification card. ➢ The system gives a verification result. ➢ The answer could be "Yes, s/he is" or "No, s/he is not.
Identification (recognition)	➢ The system gives a result whether the person being checked is registered or not. ➢ The answer could be "Yes, s/he is" or "No, s/he is not.
Source: Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000) and Hopkins, Richard, "An introduction to biometrics and large scale civilian identification" (1999) 13(3) *International Review of Law, Computers & Technology* 337-363	

In an identification system, a huge database is used to store hundreds of thousands of people's digital biometric features, whereas in a verification system, it is not necessary to have a database since the objective of such a system is to verify a person's identity, which means the registered pattern is displayed when a comparison is conducted[151]. More detailed information on how biometric systems work, is included in Appendix C.

2.8.1. *Accuracy and limits of biometric systems.* Most behavioural biometric systems are still in the testing stage, but most of physical characteristics are operational. The accuracy and effectiveness of these systems need to be checked in a real time operation environment. An essential legal concern for biometric systems is related to the level of accuracy of data.

[149] Boulgouris, Nikolaos V., *et. al*., *Biometrics, Theory, Methods, and Applications*, above n 7, p. 47.
[150] Idem.
[151] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 7, p. 9.

The biometric systems have used two performance measurements to rank the level of matching accuracy[152], known as the false rejection rate and the false acceptance rate. The first is concerned with the number of instances an authorized individual is falsely rejected by the system while the second refers to the number of instances a non-authorized individual is falsely accepted by the system[153].

For Zhang, a biometric system's accuracy is determined by combining the rates of false acceptance and false rejection. The performance of a biometric system, and therefore the false rejection rate and false acceptance rate, could be affected by[154]:

- ✓ Environmental conditions like extreme temperature and humidity
- ✓ The age, gender, ethnic background and occupation of the user
- ✓ The beliefs, desires and intentions of the user. If a user does not wish to interact with the system, then performance will be affected.
- ✓ The physical make-up of the user. A user without any limbs cannot use signature biometrics.

Hopkins claims that "[i]t needs to take into account different mechanisms for interpretation of data and different environmental conditions when the data is captured"[155]. Hopkins explains that biometric systems can present two kinds of errors or mistakes: false acceptance –when the biometric system authenticates an impostor- and false rejection –when the system rejects a valid user[156].

Fingerprints and iris recognition biometric systems are ideal for limiting entry into secured areas to known and trusted individuals. But, this biometric system is not very useful for recognizing people in public places whereas biometric facial recognition systems can recognize people at a distance, without their knowledge or

[152] Bolle, Ruud M, *et. al.*, *Guide to Biometrics*, above n 7, p. 8.
[153] Idem.
[154] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 7, p. 11.
[155] Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*",* above n 7.
[156] Idem.

cooperation[157]. More recently in the United Kingdom, as a result of threats to public safety, some public places have been heavily populated with video surveillance cameras. On average, a person moving through London is captured on video over five times a day[158]. Fingerprint systems can be used either for identification or authentication. Iris recognition is more suited for use as personal verification than fingerprints[159].

In biometric voice identification systems, there is no prior identity claim, and the system decides who the person is, or what group the person belongs to. While biometric voice authentication systems analyse an utterance from an unknown speaker and compare it with the model of the speaker whose identity is claimed. The fundamental difference between identification and authentication is the number of decision alternatives[160].

2.9. Conclusions

This chapter explored the historical background and definition in a broad sense, of biometrics. It identified that biometrics has been studied since the early 19th century, but technological advances within the ICT have revolutionised the features to generate automated systems able to collect, stored, process and exchange an impressive volume of personal data. This chapter also identified specialised authors that share a common concern in distancing themselves from a certain notion of biometrics and biometric systems, the essential feature of which is that they attempted to articulate a kind of "biometrics' knowledge". But, most of these authors do not explain relationship (or subordination) of biometrics between citizens and governments. Indeed, there are a few authors who discuss the legal impact of biometrics on privacy and data protection. Nor do these authors discuss the issues of regulation, or possible self-regulation, of the biometric industry. Moreover, the

[157] However, this biometric system is not yet perfected. Currently, some prototypes are working with free social networks, like Facebook, Windows Live, Google's Picasa and Apple's iPhoto, to be perfected for future marketing.
[158] Boulgouris, Nikolaos V., *et. al., Biometrics, Theory, Methods, and Applications*, above n 7, p. 116
[159] Idem.
[160] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 7*,* p. 180 and Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 7, pp. 48-49.

literature does not explain why biometrics has not been openly debated. A characteristic of most of these authors is that their work is written in technical terms or for a specific audience, limiting the access to "biometrics' knowledge". This chapter highlighted the need for transparency and accountability, based on Habermas and Jasanoff's theories, as part of political practice[161].

In the next chapter, the thesis analyses the biometric industry and the development of technology for the main purpose of enhancing security by identifying and authenticating individuals. In relation to privacy and data protection rights the following chapter maps out the biometric industry and explores the common practices, highlighting the importance of self-regulation. It is important to explore how far the biometric industry is willing to or can improve its self-regulation before discussion of legal problems, limitations and challenges posed by TBIF in immigration control and crime prevention contexts.

[161] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.

CHAPTER 3.

THE BIOMETRIC INDUSTRY: AN ILLUSTRATIVE MAP OF PLAYERS, PRODUCTS AND PARTNERSHIPS

3.1. Introduction

Before analysing the legal challenges of Transborder Biometric Information Flows (TBIF) there is a need to explore the biometric industry, which is responsible for rapid technological developments in automatic collection, storage, process and exchange of biometric systems. These technologies have not only transformed and expanded their original market in commercial or businesses cases, but have also diversified and intensified the use of this technology. Experts predict that this market will reach approximately USD$9,542 million by 2014[1]. This research, however, is neither about competition policies nor about patents[2].

This chapter provides an illustrative map of the industry, its players, products and partnerships. The biometric industry is evolving and expanding into different areas; developing many products and creating strategic partnerships between specialised biometric companies and other ancillary technology companies. There are biometric products developed and offered by this industry[3] that do not comply with international standards regarding encryption standard security for TBIF in the context of immigration information flow[4].

[1] Data obtained at the Welcome presentation at the Tenth ID WORLD International Congress, organised by Wise Media, in Milan, from 2nd to 4th November, 2011. However, it is possible to find various reports on the biometric market industry published by International Biometric Group, by BCC Research and by Infiniti Research Limited, but all of these reports and others are on sale online at http://www.giiresearch.com/topics/AV03_en.shtml (19/12/2012)

[2] For further details, see section 1.5. The Aim of Research.

[3] For further details, see section 3.3.2. ePassport Technology: The New Generation

[4] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

There is a lack of publicly available information about biometric industry, privacy principles, ethical commitments, current practices and regulation, apart from the information on websites and specialised magazines. In addition, there is a lack of systematic studies regarding the biometric industry itself. The absence of public debate on ethical commitments, practices and improvement for self-regulation is replicated at the international and national level. This is in contrast to the open public debates at the international and national level; on privacy and data protection positions.

The website analysis methodology was the approach undertaken for this thesis despite the limitations of such an approach. Surveys and/or face-to-face interviews might have gathered more information on the organisations; commitments and practices on the industry, however, that is not the key focus of this thesis. Nevertheless, the website search methodology did highlight an industry that is rapidly expanding, diversifying with different current practices in the four countries examples and extend their quality self-regulation and impacting significantly upon privacy and data protection rights.

Authors on Transborder Data Flows (TDF) since the 1980s have focused on electronic commerce its development, regulation, partnerships and reliability. Some authors, such as Cooper, have noted that the company, International Business Machine (IBM) clearly dominated the international computer hardware market[5] without much public debate. These authors do not centre their attention on biometric technology[6]. Nevertheless, this illustrative attempt to map the industry shows the important and continuing roles of key players of computer technology such as IBM, Hewlett Packard (HP) and Microsoft as well as new key players like Datacard Group, Safran Morpho, Gemalto, Suprema, Steria and Thales. Discourse about the relationship between citizens, government and biometric industry has been rare; with exceptions represented by Epstein and Lyon whose work discusses how biometrics

[5] Cooper, David M., "Transborder data flow and the protection of privacy: the harmonization of data protection law" (1984) 8 *Fletcher Forum* 335-352.
[6] For further details, see section 1.5. The Aim of Research

are implemented in a surveillance society. None of these authors have focused in the self-regulation in the biometric industry.

The website search on the diversification of biometric systems and current national practices in Australia, Mexico, New Zealand and Spain demonstrated not only the absence of common and clear commitment to ethical and privacy practices, but also suggested the need, in the short-term, to improve industry self-regulation. It might have been expected to find common industry codes of practice, issued by official bodies or professional associations, similar to those in other industries, such as the Payment Card Industry (PCI) and their Security Standard Council[7]. However, it was only possible to identify a specialised watchdog organisation in Australia: the Biometric Institute. The Australian Biometric Institute promotes biometric technological security standards, it has developed privacy guidelines and privacy impact assessments complying with the *Privacy Act 1988*. Members of the Biometric Institute can access annual reports online[8], but the public can only access by request.

The website search revealed two types of forums in which biometrics have been discussed. These are, first, the forums organised by the biometric industry where the discussion centres on technical issues, working more as venues for vendors. Second, the academic forums where the discussion centres on legal concerns, generally with audiences of undergraduate and postgraduate students from law and science, academic colleagues and a few public officials. These types of forums use technical terms and are for a specialised audience, limiting the access to "biometrics´ knowledge" and the level, direction and type of dialogue entered into[9]. This reflects the view of Jasanoff, who has observed that "developments suggest that some of the liveliness of contemporary democracy is to be found away from the polling booths, where one often looks for it in vain, in the less examined machinery of science and technology policy that is, in technical advisory committees, court proceedings,

[7] https://www.pcisecuritystandards.org/ (18/05/12)
[8] http://www.biometricsinstitute.org/pages/annual-reports.html (18/05/12)
[9] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* (Princeton University Press, 2007), p. 7.

regulatory assessments, scientific controversies, and even the ephemeral web pages of environmental groups and multinational corporations"[10].

This chapter argues the need to promote three types of biometric industrial guidelines: the technological security standard codes; privacy and data protection codes; and, importantly, ethical codes. Nationally or internationally, regulation should be consistent and uniform[11]. Regulation should include mutual benefits for the industry, government and society. Ideally, regulation should combine regulatory State order as well as self-regulatory biometric industry ethical and privacy codes[12]. In co-regulation and self-regulation systems the interaction between government, industry and social actors can address any possible limitations associated with direct State intervention[13]. Such approaches assist in the legitimisation on the deployment of biometric systems[14].

The fusion of biometric technology with other types of technology increases the capacity for storage of personal information. At the same time, the facilitation of information flow creates legal concerns regarding the transfer and possible misuse of information. It is important to note that these technologies are: Radio Frequency Identification (RFID), Global Positioning System (GPS) and Automatic Identification and Data Capture (AIDC). While these are mentioned at various points throughout the chapter, they are not discussed in detail[15]. They are mentioned because some biometric companies have established, as business partners, companies that develop other types of technology.

The empirical websites research provides a general map of biometric industry, classifying the companies involved in biometric technology. This chapter presents key players of biometric industry, products, commitments to ethical practices and self-regulation. The examination of commitments to ethical practices, self-regulation

[10] Idem.
[11] Black, Julia, "Constitutionalising Self-Regulation", (1996) 59(1) *The Modern Law Review* 24-55.
[12] Black, Julia, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World", (2001) 54(1) *Current Legal Problems* 103-146.
[13] Idem.
[14] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions
[15] For further details, see section 1.5. The Aim of Research

and currents practices is conducted within the framework of four countries comparative study. The chapter also assesses the diversification of biometric systems into different fields. Finally, this chapter argues the necessity to significantly improve national level co-regulation and but also self-regulation within the industry.

3.2. Mapping the Biometric Industry: Overview

Despite the absence of systematic studies on biometric industry and legal traditional sources, the empirical web research presents insights into a rapidly developing industry. This research revealed that the biometric industry consists of many companies, but relatively little is known about them or their strategic alliances with other technology industries[16] or even the developers and researchers in the biometric technology.

The website research identified that the biometric industry recognises its own weaknesses and challenges of their products not only to their clients (or potential clients) but also to people interested in their technology. This industry presents their products as effective technologies to determine identity and enhance security; and, productivity for individuals, organisations and governments. Some products may have the technical capacity to control the confidentiality and integrity of databases containing biometric information[17].

The biometric industry is a small part of the wider surveillance industry which, before 2001, was centred on the police, armed forces and other government security agencies. Before the terrorist attacks of September 11th, 2001 security was already a priority. However, after this date governments started to implement security systems

[16] The surveillance industry branched out into Radio Frequency Identification (RFID) technology, Card Technology, Global Positioning Systems (GPS) technology, Automatic Identification and Data Capture (AIDC) technology and Biometric technology.

[17] Wing, Bradford, "Future of ID, Developments in Standards & Critical Projects", in Wise Media, (Paper presented at the Tenth ID World International Congress, Milan, 3 November 2011) Wing is a Biometrics Standards Coordinator, Information Access Division - National Institute of Standards and Technology (NIST), USA.

in different areas, including immigration control[18] and crime prevention[19], which aimed to eliminate security risks by identifying individuals in an automated way.

Today biometric technology covers different market segments beyond law enforcement and security, to education, transportation (air, land and sea), banking services and financial services. Biometric technology also applies to energy, farming, agriculture, health care (pharmaceutical and medical), as discussed in the following section[20]. Acknowledging that biometrics technology has been developed to identify and authenticate individuals[21] and is used or implemented by police, armed forces and governments for security reasons, the deployment of biometric systems in different areas, including immigration and crime prevention, demands an informed public debate. This public debate should include a coordinated interaction between different actors from different areas. This interaction should involve policy makers, public officials, civil society, special advocates but also biometric industry associations. This dynamic relationship between different actors should take place nationally and internationally because biometric companies and TBIF extends beyond national borders[22].

This mapping exercise obtained information from companies' websites, but also included specialised trade magazines, information gathered at the Tenth ID World International Congress[23] and online power points presentations[24]. Basic sample information on the biometric industry was available on these official websites. The aim of the searches was to draw an indicative rather than a complete map of the biometric industry. Through these website searches, it was possible to identify 100 companies involved in biometric technology. All the companies' profiles, products

[18] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[19] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Info
[20] For further details, see section 3.3. Biometric System Applications: Diversification into Different Fields
[21] For further details, see Chapter 2. Biometric Systems: What is biometrics?
[22] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges
[23] The Tenth ID World International Congress, Milan, 3 November 2011 was organised by Wise Media.
[24] While a full analysis of the biometric industry requires specific research framework, a methodological approach and a research method, it is not the aim of this research. For further details, see section 1.5. The Aim of Research

and services were reviewed and analysed for the illustrative map of the biometric industry.

There are different ways to classify the companies that form the biometric industry. For example, one classification could be based on market segments or capitalization or size of companies or business area. However, the classification of these biometric companies, presented in this thesis is based on the products offered: specialised businesses, ancillary or mixed businesses, business partners, strategic alliances and researchers, consultancy magazines.

a. *Specialised companies.* The companies classified in this group develop and offer biometric solutions, based on the following criteria:

    1) Companies that own the most licenses,
    2) Have designed an apparatus that meets one or more standards for interoperability, and
    3) Have developed a software platform, hardware and/or application platforms.

Under these criteria, 29 companies were identified out of 100. An interesting aspect is that most of these products are offered by companies classified as strategic alliance and business partners.

It is important to note that specialised companies are small in size compared to ancillary or mixed businesses. Nevertheless, specialised companies are not local or national, but do business worldwide.

b. *Ancillary or mixed businesses.* The companies classified in this group not only develop and offer biometric solutions and comply with the criteria set out in the previous classification, but also offer other types of technology, such as smart and display cards, RFID, GPS or AIDC. An interesting aspect is that most of these companies are either part of a corporation or subsidiaries companies. Under these criteria, 20 were identified out of 100 companies.

c. *Strategic alliances and researchers.* The companies classified in this group invest in research to develop biometric technology and develop software, hardware or application platforms, but they may or may not own the license for a specific biometric technology. Under these criteria, 20 were identified out or 100 companies.

It should be noted that IBM, Microsoft and HP can be classified as business partners. However, due to the amount of biometric research carried out and the number of patents they own, these companies were classified as strategic alliances and researchers.

d. *Business partners.* The companies classified in this group develop technology cards, RFID, GPS or AIDC, but offer biometric solutions as system integrators, added value resellers or distributors. Under these criteria, 26 companies were identified out of 100.

e. *Consultancy Magazines.* The last group classification is consultancy and magazines. There are companies that offer consultation services. On one hand, this might suggest that the market is growing so fast as to allow the emergence of specific services designed to help companies make the most of their developments. On the other hand, it might simply be a limited understanding of how biometrics technology could be commercialised and how the biometric industry is developing. Company comprises those that offer news or journals both electronically and on paper. Their aims are to support the exchange of information on biometric technologies and promote their products and experience. Under these criteria, 5 were identified out of 100 companies.

The following figure shows the classification of the companies presented. More detailed information on the specialised companies, is included in the Appendix D[25].

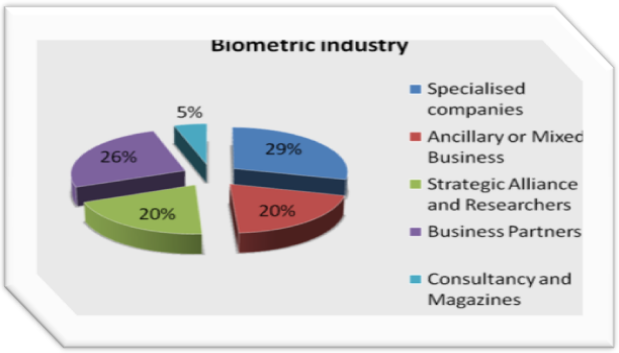
Figure 5. Biometric Industry Classification

Biometric Industry Classification				
Specialised business	Ancillary or mixed business	Strategic Alliance and Researchers	Business Partners	Consultancy and Magazines
Avalon Biometrics	Accu-Time Systems	ASK	ACIG Technologies	Cattid Sapienza
AWARE	AOPTIX Technologies	Atlantic Zeiser	Agora Bee	Global Identification
ARH	Entrust	Bundesdruckerei	Albis Technologies	HJP Consulting
Biometrics	GET Group	CSIRO	Are Con	Security solutions Magazine
Biomorf	Ghirlanda Smart Card Solutions	Datacard Group	B-Id	Wise Media
BIO-Key International	HID Global	De La Rue	Cognex	
Cognitec	Hi-Pro Solutions	Diletta	Datalogic Scanning	
Cross Match Technologies	IAI	Edaps Consortium	EBV Elektronik	
Dermalog	Infeneon Technologies	Fujitsu	Edenred	
Digital Persona	Intermec Technologies	Gemalto	Exceet Group	
Elyctis	Marketum	Giesecke & Devriet	Fasver	
ExCle	NXP Semiconductors	Hirsch Electronics	Favite	
Face First	Oberthur Technologies	HP	4P Mobile Data Processing	
Face.Com	Secunet	IBM	Identive Group	
Fingerprint Cards AB	Secure Tech Consultancy	Lockheed Martin	KSW Microtec	
Green Bit	Smartmatic	NEC	Lab ID	
Human Recognition Systems	Suprema Inc	Safran Morpho	Matica	
Identity Metrics	3M Cogent	Steria	Melzer Maschinenbau	
IdTect	Warwick Warp	Thales	Microsoft	
Intuate Biometrics	ZK Software	WWC Smart Search and Match	Murata Electronics Europe	
Iris ID			Nagra ID	
Kee Square			Osram Opto Semicondcutors	
Lumidgm			SmarTrac Technology	
Neuro Technology			RSA Security	
Pittsburgh Pattern Recognition (PittPatt)			VeriFone	
Securlinx			VPS ID	
Smart Sensors				
Speech Technology Center				
Voice Security Systems				

[25] For more information on each classification of the companies, websites, headquarters, type of technology, solutions and products, see Appendix D. List of Companies in the Biometric Industry (Complete Table)

The figure shows the average type of the companies classified under these criteria, based on the table above.

Figure 6. Type of Companies



3.3. Biometric System Applications: Diversification into Different Fields

Biometric systems were developed and mainly implemented for law enforcement activities, security and forensic science, but these systems have now been applied in other fields as well[26]. This section discusses the deployment of biometric systems in different areas in order to enhance security and solve identity-related problems.

The implementation of biometric systems is often called biometric technologies and these, in turn, are diverse and expanding.

> "The increased prominence of social control via engineering is related to concerns over issues such as crime, terrorism, drug abuse, border controls, AIDS, and economic competitiveness; and to technical developments in electronics, computerization, artificial intelligence, biochemistry, architecture, and materials science. The scale, mobility, and anonymity of mass society and ironically, increased expectations of and protections for privacy, have furthered reliance on external, impersonal, distance-mediated, secondary technical means, and database memories that locate, identify, register, record, classify, and validate or generate grounds for suspicion. The perception of catastrophic risks in an interdependent world relying on

[26] For further details, see Chapter 2. Biometric Systems: What is Biometrics?

complex technologies and the entrepreneurial efforts of the security industry and governments such as the United States with its war on drugs, have helped spread the technologies internationally"[27].

As noted there is a lack of publicly available systematic studies on the biometric industry that explain and assess the expansion and diversification of the biometric technology. This research relies on the technical specialised literature that promotes the implementation of this technology in the variety of applications, ranging from healthcare to banking services, immigration to public transportation, and private and public security. Theoretically, this specialised literature has no consensus on classification of biometric systems. For some authors[28] the classification should be based on purposes and limits of biometric systems[29], identification and authentication, where others consider that classification should be based on biometric systems applications[30]. The specialised literature that supports the classification based on biometric systems applications has developed four categories of classification. The first system category is that of controlling access to data, such as logging onto a device or a network; the second is that of controlling access to tangible materials or areas, such as physical access control; the third category is validating a claimed identity against an existing credential, as happens in a border control environment; and the fourth is registering or identifying individuals whose identities need to be established biometrically, most often using centralised or distributed databases[31].

To illustrate this diversification and expansion of biometric industry in everyday life of the popular fields, where it is possible to find the deployment of biometric systems can be presented. These are: law enforcement, banking, computer networks,

[27] Marx, G.T., "Technology and Social Control", *International Encyclopaedia of the Social & Behavioural Sciences*, (Elsevier, 2001), pp. 15506-15512.
[28] Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000); Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003); Bolle, Ruud M., *et. al*., *Guide to Biometrics*, (Springer, 2003).
[29] For further details, see section 2.8. Purposes and Limits of Biometric Systems
[30] Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Day, David, "Biometric Applications, Overview", *Encyclopaedia of Biometrics,* (Springer, 2009). http://springerlink.metapress.com/content/q22t17844168/fulltext.pdf (18/12/2012)
[31] Idem.

physical access, benefit systems or social programmes, immigration and border control, national identity cards, telephone systems, and employment, among others.

a) *Law enforcement.* Over the last 60 years, biometrics has been in law enforcement but the role of biometrics has expanded into a wide range of applications in the private sector. The law enforcement field is perhaps the largest biometrics user group. Biometric systems have been used as surveillance systems. An individual's fingerprints are used to determine or confirm the identity of people of interest[32].

Another use can be found in the forensic identification of suspects, convicts and victims in disasters by using DNA[33].

> "In the UK, the recognised 'world leader' in forensic DNA databases, the criteria for inclusion has advanced from those people convicted of a crime, to those charged, and then in 2004, simply to those arrested. On an international level, talks about increasing cooperation in the areas of security, law enforcement, and policing, include the idea of exchanging DNA data"[34].

b) *Banking.* According to Zhang and Day, banks have been testing a range of biometrics technologies for many years. Emerging markets such as telephone and Internet banking must also be completely secure for clients and bankers alike. A variety of biometric technologies are now striving to prove themselves in this diverse market opportunities national and global banks[35].

---

[32] The FBI currently holds one of the largest biometric databases, comprised of tens of millions of civilian and criminal fingerprint records. Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 28, p. 14; Day, David, "Biometric Applications, Overview", above n 30.

[33] Since 1988, the European DNA Profiling Group (EDNAP) established systematic procedures for data-sharing across the European community. The main purpose of the Standardization of DNA Profiling in the European Union (STADNAP) group is to promote cooperation across the European Union in order to utilise DNA profiling to detect "mobile serial offenders". The European Network of Forensic Science Institutes (ENFSI) has similar ambitions to standardise forensic practices in support of policing across the entire European Union. Van Der Ploeg, Irma, "Genetics, biometrics, and the informatization of the body" (2007) 43(1) Ann Ist Super Sanità 44-50.

[34] Idem.

[35] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 28, p. 13; Day, David, "Biometric Applications, Overview", above n 30.

c) *Computer networks.* Biometrics is commonly used to control access to centralised databases of healthcare information or financial records. Biometric technologies are proving to be more than capable of securing computer networks. This market area has phenomenal potential, especially if the biometrics industry can migrate to large-scale Internet applications[36].

d) *Physical access.* Offices, schools, hospitals and military facilities around the world are implementing biometric systems in place of old fashioned key codes to minimize security threats. The potential applications are infinite. Cars, buses and houses, for example, are under the constant threat of theft and biometrics could offer the perfect security solution[37].

e) *Benefit systems.* Benefit or social systems like welfare especially need biometrics to fight fraud and ensure payment to the correct person[38].

f) *Immigration and border control.* For immigration and border control authorities around the world it is essential to quickly and automatically process lawful travellers and identify law breakers[39]. The International Civil Aviation Organization (ICAO) adopted a global blueprint to integrate biometrics into machine readable travel documents[40].

g) *National Identity.* Biometrics are beginning to assist governments as they record population growth, identify citizens and prevent fraud from occurring at local and national elections. Finger, face and signature biometric recognition systems are particularly strong in this area and plans to implement this technology are already underway in Colombia, Jamaica, Lebanon, India, Mexico, the Philippines, South Africa, Spain, Germany and Poland, among other countries[41].

---

[36] Idem.
[37] Idem.
[38] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 28*,* p. 14.
[39] Ibidem*,* p. 14 and 15; Day, David, "Biometric Applications, Overview", above n 30.
[40] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[41] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 28*,* p. 15.

h) *Telephone systems.* Global communication has expanded over the past decade. Telephone companies are concerned about fraud and biometric systems are considered. Speaker ID is well-ranked to the telephone environment and is making inroads in these markets[42].

i) *Employment.* Biometric systems technologies are used to carry out background checks as a condition of employment in many government agencies and the private sector. Generally, it can also be used to track employee attendance and work patterns[43].

These examples demonstrate the diversification and expansion of biometric technology, but also raise basic questions on how both the private and public sectors have adopted this technology; how the implementation of biometric technology and TBIF fit into the broader international framework and national regulation; and, how self-regulation instruments are needed in this industry. It is important to note, however, that the implementation of biometrics in the private sector is beyond the parameters of this thesis. Public process should be coordinated by governments to address those questions by balancing public interests, on security and national defence with individuals' privacy and data protection rights. This type of public process should be accompanied with the creation of new patterns of interaction between social actors, biometric industry and government. These public processes cannot and are not intended to prevent the development of biometric technology but to legitimise the implementation of biometric technology and TBIF, in immigration control and crime prevention in particular. Governments cannot assume that they have a monopoly on the exercise of power and control[44]. In addition, legislators can use these processes to address technological legal issues of co-regulation and encouraging self-regulation[45].

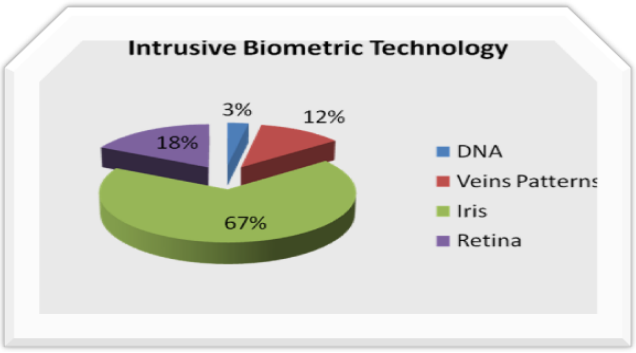
[42] Idem.
[43] Idem; Day, David, "Biometric Applications, Overview", above n 30.
[44] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia*)", Cultura e Critica*, (Einaudi, 1980).
[45] For further details, see section 3.5. Development of Self-Regulation in the Biometric Industry

3.3.1. *Products Developed by the Biometric Industry*. This section identifies the most popular or common biometric products developed and offered by the biometric industry. From the 100 companies classified, 53 are directly involved in developing biometric technology as specialised businesses, ancillary or mixed businesses and strategic alliances and researchers.

These companies develop intrusive (DNA, veins patterns, iris and retina patterns) and non-intrusive (fingerprints, palmprints, facial recognition, signature and voice) biometrics technology. For full information on biometrics typology, see Appendix B[46]. It has been possible to identify the development of other behavioural biometric technology. More information on these companies and their biometric products and solutions, are included in Appendix D[47].

The most common or popular biometric technology products offered are for fingerprints with 43 companies; facial recognition with 38; iris recognition with 23; and, palmprints with 19 companies. The following charts show the average type of intrusive and non-intrusive biometric technology products.

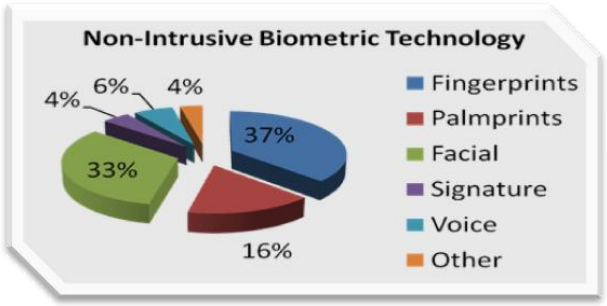
Figure 7. Intrusive Biometric Products



The iris and retina recognition systems are the most common intrusive biometric technology available on the market. Fingerprints and facial recognition are the most common non-intrusive biometric technology available on the market.

[46] For further details, see Appendix B. Biometrics Typology
[47] For further details, see Appendix D. List of Companies in the Biometric Industry (Complete Table)

Figure 8. Non-Intrusive Biometric Products



It is important to note that most biometric software solutions have been compiled for the most common platforms like Windows XP, Windows Server Applications, Windows CE or Linux. Most of the companies specialising in smart cards or electronic ID (eID) comply with international security standards[48] like American National Standard Institute (ANSI), National Institute of Standards and Technology (NIST) and International Civil Aviation Organization (ICAO), according to their websites.

3.3.2. *ePassport Technology: The New Generation*. The biometric industry merges and evolves to meet market expectations with its technological innovations. National governments plan for these services with a view to the mobility of their resident populations.

The challenge that the biometric industry faces regarding travel documents (passports and visas) is to select and design a secure travel document with the right mix of quality, security, durability and cost to manage risks[49]. Habermas and Jasanoff[50] theories argue that it is possible to legitimise political policies on the implementation and deployment of this technology through the participation of citizens. Jasanoff argues that "the visibility and influence of each actor type varies from country to country, as do their institutional resources and opportunities to

[48] Standards are requirements for interoperability between dissimilar systems and exchange encrypted information to avoid the disclosure of personal information, including biometric information.
[49] Nick Nugent, "High Security Identification Documents Using QSDC to Determine the Right Mix" (Paper presented at the Tenth ID WORLD International Congress, in Milan, 4 November 201).
[50] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia*)",* above n 44.

participate in political debate"[51]. This became relevant when governments select or choose the specialise company for travel documents, such as ePassports.

The production and issue of passports and visas involve specialised businesses or ancillaries or business partners, such as booklet producers, inlay manufacturers, chip makers, standardization manufacturers, high security paper manufacturers and security printer makers, among others. There are three mandatory types of electronic passport (ePassport) generations according to the International Civil Aviation Organization (ICAO)[52]: biometric passports with Basic Access Control (BAC); biometric passports with Extended Access Control (EAC); and, biometric passports with Supplemental Access Control (SAC). These ePassports are known as Machine-Readable Travel Document (MRTD) embedded with a secure element based on the specifications defined by the ICAO. All ePassports have a contactless microprocessor chip on which information about the passport holder is stored. This may include biographic data such as name, date and country of birth, medical information and a facial image of the passport holder[53]. A contactless enabled reader is used to read this data from the passport.

Figure 9. Biometric Passport[54]

[51] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9, p. 29.
[52] The ICAO is a specialised agency of the United Nations created in 1944 to promote the safe and orderly development of international civil aviation throughout the world. The ICAO *Machine Readable Travel Documents, DOC 9303* is divided into three parts with their respective volumes. The specifications are located in Part 1, Volume 2, which states that MRTD must be used to conform to ICAO's globally interoperable requirements and qualify as a *true 'ePassport. ICAO Machine Readable Travel Documents, DOC 9303,* (Pt 1, 6th ed, 2006) vol. 2 http://www.icao.int/publications/pages/publication.aspx?docnum=9303 (19/12/2012)
[53] A facial image of the passport holder is mandatory according to ICAO specifications. Idem.
[54] Image from the Bundesdruckerei website http://www.bundesdruckerei.de/en/1205-epassport-id3 (19/12/2012) this company has been identified in this chapter.

These are new generation ePassport with chip stores of both demographic and biometric data. Biometric data may include fingerprints, iris patterns or other biometric data (optional according to ICAO specifications) and facial biometric image (mandatory according to ICAO specifications):

a) Biometric passports with Basic Access Control (BAC). The BAC is a mechanism that was introduced to ensure that the biographic data and facial imaged stored on the ePassport microprocessor chip is read securely. Australia[55] and New Zealand[56] issue this type of passports.

b) Biometric passports with Extended Access Control (EAC). These are the second generation biometric passports. The EAC is a mechanism that restricts access to highly sensitive biometric data, including both optional and mandatory biometric characteristics. This ePassport is based on asymmetric cryptographic protocols and uses stronger encryption.

c) Biometric passports with Supplemental Access Control (SAC). These are the third generation biometric passports. The SAC is a Password Authentication Connection Establishment (PACE) that restricts access to highly sensitive biometric data more, including optional and mandatory biometric characteristics. It implements asymmetric cryptographic and bases data encryption on a key shared between the reading device and the chip. Spain will issue this type of passport[57].

[55] Australia began issuing October 2005 https://www.passports.gov.au/web/epassport.aspx (19/12/2012)
[56] New Zealand began issuing September 2005 http://www.passports.govt.nz/ (19/12/2012)
[57] Spain began issuing biometric passport with Basic Access Control (BAC) since July 2003. However, in December 2014 Spain will began issuing biometric passport with Supplemental Access Control (SAC) http://www.policia.es/documentacion/docu_esp/pasaporte/concepto_pas.html (19/12/2012) http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/document-security/docs/comm_decision_c_2013_6181_en_.pdf (27/10/2013)

It was not possible to identify the type of access control of Mexican biometric passports. The publicly available information specified that Mexico began issuing biometric passport at the end of 2012[58] with an electronic bar code and a hologram picture of the holder in the centre right. The front cover of a Mexican biometric passport does not have the symbol of the contactless microprocessor chip on the front page of the passport. The company which won the nationwide passport project in Mexico was Suprema Inc[59].

A significant finding of this websites research was that, of the 100 companies identified on the mapping biometric industry[60], only 50 companies described themselves on their websites as suppliers of ePassport technology. But, comparing these 50 companies and their products against ICAO's specifications the result was that not all companies fully meet the terms established by ICAO[61]. Only 19 companies of 50 that announced themselves as suppliers of ePassport technology comply with ICAO´s requirements. This is critical considering that governments as clients of these companies rely on their expertise and knowledge of biometric technology in general and ePassport technology in particular. There have been biometric passports of different countries that fail the test performance and the test of operational impacts of processing ePassports on the primary inspection process[62]. This raises three main questions about the ethical commitment; current practices and the quality of self-regulation of biometric industry.

The following figure shows the companies that are authorized to supply the mandatory ICAO components, equipment, information technology and services for issuing ePassports.

---

[58] Mexico began issuing November 2012 http://www.sre.gob.mx/index.php?option=com_content&view=article&id=242&Itemid=264 (21/07/2013)

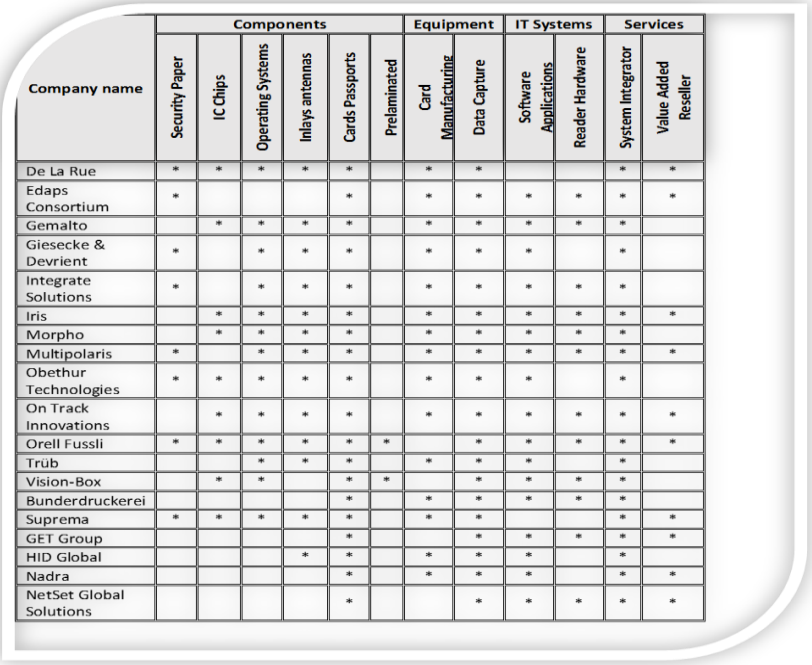
[59] This company has been identified in this chapter http://www.supremainc.com/eng/news/press.php?mark=1&bbs_no=11372&bbs_code=10001&symode=view (21/07/2013)

[60] For further details, see section 3.2. Mapping the Biometric Industry: Overview

[61] *ICAO Machine Readable Travel Documents, DOC 9303,* above n 52.

[62] Wing, Bradford, "Future of ID, Developments in Standards & Critical Projects", above n 17. Wing is a Biometrics Standards Coordinator, Information Access Division - National Institute of Standards and Technology (NIST), USA.

Figure 10. ePassport Industry



Company name	Components						Equipment		IT Systems		Services	
	Security Paper	IC Chips	Operating Systems	Inlays antennas	Cards Passports	Prelaminated	Card Manufacturing	Data Capture	Software Applications	Reader Hardware	System Integrator	Value Added Reseller
De La Rue	*	*	*	*	*		*	*			*	*
Edaps Consortium	*				*		*	*	*	*	*	*
Gemalto		*	*	*	*		*	*	*	*	*	
Giesecke & Devrient	*		*	*	*		*	*	*		*	
Integrate Solutions	*		*	*	*		*	*	*	*	*	
Iris		*	*	*	*		*	*	*	*	*	*
Morpho		*	*	*	*		*	*	*	*	*	
Multipolaris	*		*	*	*		*	*	*	*	*	*
Obethur Technologies	*	*	*	*	*		*	*	*		*	
On Track Innovations		*	*	*	*		*	*	*	*	*	*
Orell Fussli	*	*	*	*	*	*		*	*	*	*	*
Trüb			*	*	*		*	*	*		*	
Vision-Box		*	*		*	*		*	*	*	*	
Bunderdruckerei					*		*	*	*	*	*	
Suprema	*	*	*	*	*		*	*			*	*
GET Group					*			*	*	*	*	*
HID Global				*	*		*	*	*		*	
Nadra					*		*	*	*		*	*
NetSet Global Solutions					*			*	*	*	*	*

According to ICAO's report, over 104 countries distribute ePassports[63]. It is important to highlight that the ICAO published a supplement to Doc 9303 in October of 2013[64]. This supplement does not replace DOC 9303, but updates, clarifies and incorporates new technologies and solutions into ePassports.

Besides the issue of ePassports, national governments are deploying a border management systems to address illegal immigration, cross-border criminals and terrorist threats. Both the implementation of border management systems and the deployment biometric databases are measures that limit the rights of privacy and data protection[65]. These issues will be discussed in greater detail in a later chapter[66].

[63] ICAO, "The Implementation of ePassports", *MRTD Report No. 3* (2012) http://www.icao.int/publications/journalsreports/2012/MRTD_Report_Vol7_No3.pdf (19/12/2012)
[64] *ICAO Machine Readable Travel Documents, DOC 9303,* above n 52.
[65] For further details, see section 1.4 Hypothesis
[66] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow and Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

3.4. Industry Commitment to Ethical Practices

The biometric industry makes claims to a commitment to ethical, legal and self-regulation practices. The biometric industry develops technology that may undermine privacy and civil liberties, hence the importance of identifying whether this industry is in actual practice committed to ethical practices. Through the website search, it was possible to identify this industry commitment in three categories, namely extracts of ethical codes; extracts of privacy and data protection codes or guidelines; and, references to white papers[67].

It is important to note that 74 were identified out of 100 companies provide a section on their websites related to terms and conditions, legal notices on privacy and data protection policies regarding its customers' privacy and personal data. These 74 include a range of companies from specialised to ancillary business, a small number of strategic alliances, a small number of business partners, and, some consultancy companies. This may be interpreted as a misunderstanding of concepts related to terms and conditions with ethical codes; with privacy and data protection policies and confidentiality for clients. A small number of companies, most of them classified as strategic alliances and business partners[68], had sections on ethical practices and corporate responsibilities, (Edaps Consortium, Gemalto, HP, IBM and Microsoft), but these sections are broad, nonspecific and vague. Corporate responsibilities statements are limbed to self-regulation but in the absence of a professional associations or an impartial body to supervise these companies globally, these statements are not actionable. However, it is noted that these companies embrace ideas of social good and responsibility for their actions[69].

[67] White papers are guides that help to understand an issue, solve a problem or make a decision.
[68] For further details, see section 3.2. Mapping the Biometric Industry: Overview
[69] For further details, see section 3.5. Development of Self-Regulation in the Biometric Industry

Only three companies give specific details on their commitment to practices in relation to privacy and civil liberties: IdTect and Digital Persona, classified as specialised business, and HID Global, classified as ancillary[70]. On its website, IdTect states that: "Our idEye software can be customized to suit individual client's requirements, and it also complies with all privacy legislation principles"[71]. Digital Persona mentions 10 white papers on access control and data encryption[72]; perhaps, the most important of which is about complying with data breach notification laws. This white paper explains the potential economic effects of security breaches of personal identifiable information by theft or unauthorised access and proposes technological security solutions[73]. The company HID Global has 40 white papers covering most of their products[74], with the most relevant about access control best practices[75]. This white paper offers a choice on the use of a secure protocol to protect stored personal information and protect cross-border communications. However, these examples of commitment to privacy practices are not industry standards and do not meet any rigorous analysis from a human rights perspective.

In summary, the biometric industry is rapidly evolving and is gaining a presence in different fields. Some preliminary conclusions can be drawn in terms of ethical commitments. It is possible that the biometric industry is confused on the use of the terms privacy and confidentiality. There is a lack of a common and widespread interest to engage with ethical commitments or corporate responsibilities. In addition, the research identified companies that declare themselves as suppliers of ePassports technology but fail to meet ICAO's specifications; this situation raises concerns about the quality of self-regulation. Society and government trust in these private enterprises and its technology. Further legal research is needed to explore

[70] For further details, see section 3.2. Mapping the Biometric Industry: Overview
[71] This company has been identified in this chapter. http://www.idtect.com.au/ (19/12/2012)
[72] This company has been identified in this chapter http://www.digitalpersona.com/resources/case-studies_white-papers/ (19/12/2012)
[73] http://www.digitalpersona.com/uploadedFiles/Collateral/White_papers/WP_Compliance_DataBreach_20100831.pdf (19/12/2012)
[74] This company has been identified in this chapter http://www.hidglobal.com/document-library?field_category_tid_i18n=All&field_brand_tid_selective=All&field_document_type_tid_selective=711 (19/12/2012)
[75] http://rs-test.hidglobal.com/sites/hidglobal.com/files/resource_files/hid_global_best_practices_in_access_control_white_paper_04-20-2012.pdf (19/12/2012)

self-regulation and market dominance, as these issues are beyond the parameter of this thesis[76].

3.5. Development of Self-Regulation Standards in the Biometric Industry.

Regulations consist of a set of legal rules that establish rights and legal duties of persons in the scope and limits of their activities, generally enacted by legislatures. By contrast, self-regulation is the control of actions independently of legislative and governmental supervision. This independent supervision should be often undertaken by professional associations, in this case the biometric industry itself. Finally, a combined system, where both "regulation" and "self-regulation" coexist (co-regulation[77]) involves certain advantages for the biometric industry. Regulation encourages the participation of government bodies and feedback between different sectors of society. The most important issue in a self-regulatory model is the existence of mechanisms that limits government intervention. The legitimacy of the self-regulation model for the biometric industry implies a commitment to carry out activities that involve the values and ethical recognition from society. However, self-regulation can fail as it does not involve any penalty or sanction. The effectiveness of self-regulation depends on public opinion and public confidence[78].

The aim of the regulation, on the other hand, is to create the minimum legal principles necessary in a democratic constitutional State[79]. Regulation is directed at the industry and not at the technology itself. Self-regulation for the biometric industry itself aims to achieve the highest possible quality of practices through the continuous feedback of activists and academic experts, especially in the field of privacy and data protection. A generic definition of the idea of self-regulation has been offered by the United States Department of Commerce:

[76] For further details, see section 1.5. The Aim of the Research
[77] Black, Julia, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World", above n 12.
[78] Braithwaite, John, "Responsive Regulation in Australia" in Grabosky, Peter y Braithwaite John (eds.), *Regulation and Australia's Future*, (Australian Institute of Criminology, 1993), p. 81-88; Doyle, C., "Self Regulation and Statutory Regulation" (1997) 8(3) *Business Strategy Review* 35-42.
[79] For further detail, see section 1.8.3. Theoretical Approaches

> "Most basically, we need to define what we mean, as the term "self-regulation" itself has a range of definitions. At one end of the spectrum, the term is used quite narrowly, to refer only to those instances where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the need to regulate itself for whatever reason— to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputation, or to level the market playing field— and does so"[80].

The combined or mixed system, known as co-regulation is the better solution for an industry that is expanding and evolving rapidly. Co-regulation is a mechanism of sharing responsibility between governments, society and the biometric industry. Self-regulation has the strategic problem of the voluntary will of biometric companies to meet best practices. One failure by a biometric company can expose and affect the reputation of the whole biometric industry[81]. In a co-regulation system the strategy is to determine a structured cost benefit approach to policy development to identify whether the proposed regulation meets the dual goals of "effectiveness" and "efficiency"[82] creating mutual benefits for biometric industry, government and society. Thus, the resolution of problems of ethical commitments, corporative responsibilities and breaches of rights should be governed by both the regulatory system and the self-regulation system[83]. These are not exclusive or antithetical systems, on the contrary, they complement each other.

Within a co-regulation system or self-regulation system, the biometric industry should create open global forums to discuss ethical practices; corporate responsibilities; and, compliance with privacy and data protection laws. There is, arguably an

[80] United States Government, United States Department of Commerce, National Telecommunications and Information Administration, *Privacy and Self-regulation in the information age*, (1997).
[81] However, pure government regulation also has strategic problems: regulation can be impede the development of the biometric industry; there may be conflicts of interest when the biometric technology is deployed in public sector; and, the legislative process can take a considerable time compared with the rapid changes in biometric technology. Black, Julia, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World", above n 12.
[82] Office of Regulation Review 1998, *A Guide to Regulation (second edition).*
[83] Black, Julia, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World", above n 12.

absence of these types of forums, with little public discussion about the introduction of biometric technology and a lack of publicly available information on the deployment of biometric systems and TBIF in the context of immigration information flow and information flow in criminal databases[84]. For Spain, as a European country, the *Directive 95/46/EC* sets an article where the Member Countries shall encourage the draw up of a code of conduct[85]. Nevertheless, only Australia from the four countries study has a professional body that has made efforts to promote an effective and appropriate use of biometric technology.

3.5.1. *Biometric Industry Self-Regulation: Professional Associations in Australia.* The four countries study revealed one organisation that has made modest and impartial efforts in the biometric industry, the organisation Biometric Institute.

The Biometric Institute, an Australian based non-profit organisation, proposed its *Biometric Institute Privacy Code*, in 2006, with recommendations based on National Privacy Principles and the *Privacy Act 1988*[86]. Companies like Unisys, Identix and Argus Solutions are members of the Biometric Institute. However, this Biometric Institute Privacy Code was revoked by the Australian Privacy Commissioner on 2012 because of "the Code only binds the members of the Institute that subscribe to the Code. There have been low members of subscribers to the Code. This was cited by the Biometrics Institute as a reason for seeking the revocation of the Code"[87]. In addition, in the Biometric Institute website sections of 'annual reports' and 'resource library' are only available to members, who apply, pay and become a member. Significantly research articles; government reports; white papers; and, vendor reports are not publicly available. This Biometric Institute is not a significant body in

[84] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9; and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia*)",* above n 44.
[85] Article 27 EU *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.*
[86] Most of its members are Australian users and industry. Although its members primarily are form Australian and New Zealand its goal is to include members from the entire Asia Pacific region. The Biometrics Institute industry members include Unisys, Identix and Argus Solutions. For further Biometric Institute information see http://www.biometricsinstitute.org/ (19/12/2012)
[87] Under the *Privacy Act 1988,* the Australian Privacy Commissioner can approve codes of practice about personal information. Explanatory Statement, *The Privacy Act 1988* (Cth) 1-5, 4 http://www.comlaw.gov.au/Details/F2012L00869/Explanatory%20Statement/Text (19/12/2012)

spreading public debate, transparency and accountability in the deployment of biometric technology and TBIF in Australia.

3.6. Current Practices of the Biometric Industry in Different Countries

This section examines four countries examples of the current applications of biometric technology in different fields and biometric industry practices. Mapping the biometric industry illustrates not only the key players, products and partnerships, but also opens a global window on the current practices and ethical commitments of this industry. These country examples, two Common Law countries and two Civil Law countries, reveal the approach legal challenges in biometrics technology in a proportional way. In addition, these examples present the impact on privacy and data protection rights in the four countries: Australia, Mexico, New Zealand and Spain[88].

3.6.1. *Australia: Database IdEye Implemented in Pubs and Clubs.* The company Idtect[89] is an Australia specialised company that developed ID scanning software with two software identification tools: "Alcohol Management Systems" and "idEye for clubs and pubs". This research will focus its attention on the idEye for clubs and pubs.

In Australia, the private sector is covered by the *Privacy Act 1988* and must comply with the *Australian Privacy Principles* (APPs) in handling personal information. Under the *Privacy Act 1988* the Federal Privacy Commissioner does not have a complete jurisdiction to audit private sector systems[90]. But, in 2010 guidelines for private sector hospitality organisations were drawn up by the Federal Privacy Commissioner[91] for pubs and clubs that demand an ID. Some pubs and clubs also demand biometric photos and fingerprints of every individual who enters. Idtect

[88] For further details, see section 1.3. Country Profiles for the Comparative Study Component
[89] This Company has been identified in this chapter http://www.idtect.com.au/ (19/12/2013)
[90] On 1 November 2010 the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner. In 2014, important changes to the *Privacy Act 1988* commence into force http://www.oaic.gov.au/ (19/12/2013)
[91] Office of the Privacy Commissioner of Australia, *Private sector information sheet 30 – ID scanning in pubs and clubs*, (April 2010) http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-30-2010-id-scanning-in-clubs-and-pubs (19/12/2013)

scanners scans identities onto a database, called “the ban list” which is shared on local, state or national levels. The system stores the data for a month and then deletes it, but any troublemaker’s personal information can be kept indefinitely. In this case, the argument used to justify the implementation of this technology is that “public safety should over rule issues about privacy”. In this scenario, the information collected does not reveal sensitive personal information. However, the collection of photographs, fingerprints and driver licences raises concerns about unauthorised access, misuse, identity fraud and disclosure of information.

First, under 2010 guidelines for private sector hospitality organisations, individuals must be notified what will happen to the information collected at pubs and clubs: the purpose of the collection, with whom they will exchange this information, who will have access to it and when the information will be destroyed.

Second, based on the characteristics of the venues and the software identification idEye the information may be stored on their servers as a backup. When the venue shares or collects from third parties, the information is stored on the database located in each venue’s network servers or even on a private cloud. Under the *Privacy Act 1988* and the *National Privacy Principles*, venues must have robust security measures that protect information, but they also must ensure that personal information is accurate and up-to-date.

It is important to highlight that biometric information must be collected for valid reasons, in this case, valid business reasons. The most interesting legal concern is that regarding the ban list. The ban list means that individuals banned at one location may be refused entry at other venues. The individual on that biometric database is flagged and venues may choose to accept or ban him or her. Venues impose bans for a discretional period of time: a day, a month, a year or indefinitely. This ban list database infringes, on one hand, civil liberties since the disclosure of the ban list could cause discrimination. On the other hand, the existence of a ban list where cancelation of personal information is discretional; this clearly undermines privacy and data protection rights. This discretional period of time consists in transgression to “the right to be forgotten or the right to withdraw their consent to data processing”

and it is consistent with Castellano that explains the “right to be forgotten” as an element of the right of data protection (self-determination) when the owner of the data has withdrawn his/her consent for processing or when he/she objects to the processing of his/her personal data[92].

It can be argued that the discretionary power to ban people could be the result of a proactive society in activities in which government has a security and protection role in fighting violence in pubs and clubs. However, the State has responsibilities in the use of such technologies.

> “Although individual interests must on occasion be subordinated to those of a group, democracy does not simply mean that the views of a majority must always prevail: a balance must be achieved which ensures the fair and proper treatment of minorities and avoids any abuse of a dominant position”[93].

The State should not be passive towards transgressions against civil liberties and rights. So Valades has stated that, “if the violation of one of those rights and freedoms is the result of a breach of that duty in terms of national legislation, the State is ultimately responsible for any violation”[94].

3.6.2. *Mexico: Fingerprint Implemented at Banco Azteca.* The company Digital Persona[95] is a U.S. specialised business that develops biometric fingerprint products for two applications: customer authentication for secure banking and credit

[92] This has been developed by Spaniards authors and recently promoted to the European Commission. Simon Castellano, Pere, "Los límites jurídico-constitucionales de la Administración electrónica en España y el Open government" (2011) 27 *Revista Aranzadi Derecho y Nuevas Tecnologías* 67; *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [2012] COD 2012/0011.

[93] Young, James and Webster v *United Kingdom* (European Court of Human Rights, Plenary, Application Nos 7601/76 and 7806/77, 13 August 1981) 63.

[94] Valades, Diego, “La Protección de los Derechos Humanos Frente a Particulares” in Bogdandy Armi von, Ferrer Mac-Gregor, Eduardo and Morales Antoniazzi, Mariela (coords) *La Justicia Constitucional y su Internacionalizacion. Hacia un Ius Constitucionale Commune en America Latina?,* (UNAM, Instituto Iberoamericano de Derecho Constitucional, Max-Planck-Institut Für Ausländisches Öffentliches Recht Und Völkerrecht, 2010), pp. 681-710.

[95] This company has been identified in this chapter http://www.digitalpersona.com/ (19/12/2012)

transactions, and employee authentication for branch executives, tellers and vault access.

In 2002, Banco Azteca[96] started operations targeting the low income sector, which represents the 70% of population not served by traditional banks. In addition, Banco Azteca became the first bank to implement biometric fingerprints as a method to protect customers' savings in a product called "Guardadito" (saving accounts). At that time, Mexico neither had a data protection law nor a Data Protection Commissioner.

In Mexico, recognizing data protection as a fundamental right has been a gradual process. This process started in 2007[97] and in 2010 the *Federal Data Protection for Private Sector Law* was approved. This law came into force in January 2012. Under the *Federal Data Protection for Private Sector Law*, all private sector entities, including banks, must notify individuals about their information collected on their websites: the purpose of said data collection, with whom the information will be exchanged, who will have access to said information and when this information will be destroyed[98].

In 2007 any movement of money through bank portals had to be confirmed by a dynamic passwords device; thus Banco Azteca expanded the use of biometric fingerprints to customers' financial and banking services, to secure employee access to bank vaults and to time attendance control[99]. There were two companies involved

[96] Banco Azteca is a subsidiary of Group Elektra, a Mexican financial and retail corporation owned by Grupo Salinas. Currently, Banco Azteca has holdings in Panama, Honduras, Guatemala, El Salvador, Peru and Brazil. http://www.bancoazteca.com.mx/PortalBancoAzteca/publica/conocenos/historia/quienes.jsp (19/12/2012) (information in Spanish)

[97] Since 2000, several bills have been presented without coming to any fruition. In 2007, The Federal Congress approved an amendment to Article 6 of the Constitution which recognizes and gives content to the right to data protection. The amendment reflected the rights that holders have over this type of data, such as those of access, rectification, cancellation and objection (known by its acronym in Spanish as ARCO rights). This is highly significant considering that personal data are in the hands of governments and the private sector (companies, organisations and professionals).

[98] http://www.bancoazteca.com/PortalBancoAzteca/publica/conocenos/historia/AvisoPrivacidad.htm (19/12/2012)

[99] Customers can acquire a fingerprint reader from the bank and plug it into their computers for $55 AUD plus tax ($742.40 Mexican pesos) and the software can be downloaded from Banco Azteca's website.

in the biometric applications: Biometria Aplicada[100], a reseller, and Digital Persona. Furthermore, Banco Azteca plans to incorporate biometric fingerprint readers into its ATM machines for customers to check their balances, withdraw cash or purchase pre-paid mobile phone minutes. Banco Azteca requests an official identification card with the holder's current address, email address, personal information and one biometric fingerprint. The information collected does not reveal sensitive personal information. However, many customers are farmers and construction workers whose fingers are damaged and worn.

Based on bank characteristics, the information is stored on different databases where distributed database management is required. The information is stored on multiple network servers. This gives banks the ability to link the different databases of each location and gain access to bank branches.

It is important to highlight that it has only been two years since the data protection law has come into force. Thus, there are no complaints against Banco Azteca or appeals yet to be solved by the Federal Privacy Commissioner[101] whereas at the National Commission for the Protection and Defence of Users of Financial Services, it is ranked number one in the 2011 Index of Fines[102]. It will be a matter of time to find out whether Banco Azteca is complying with the data protection regime. The Federal Privacy Commissioner has that authority to audit their databases and, in case of irregularities, to impose a corresponding sanction.

3.6.3. *New Zealand: Biometric Voice Recognition.* The company Salmat[103] is a specialised Australian company that provides customer communication solutions. It has developed three Voice ID versions: one similar to the interactive voice response system, an online identification system and a mobile identification system, all of

[100] This company has been identified in this chapter. http://www.biometriaaplicada.com/ (19/12/2012)
[101] Freedom of Access Information and Data Protection Institute (known by its acronym IFAI) http://www.ifai.org.mx/English (19/12/2012)
[102] Mexico Government, National Commission for the Protection and Defence of Users of Financial Services, *Fines imposed on financial institutions,* (2012) http://www.condusef.gob.mx/PDF-s/Comunicados/2012/com05_multas-2011.pdf (19/12/2012)
[103] This company has been identified in this chapter http://www.salmat.com.au/ (19/12/2012)

which use biometrics[104]. The voice identification biometric systems are inexpensive and good for remote database access, but it can be affected by physical conditions or emotional states.

In 2008, New Zealand's Inland Revenue (IR)[105] began to modernise its phone interface. In November 2011, IR implemented Salmat Voice ID[106] as its interactive voice response system. This voice ID allows taxpayers to access their accounts by telephone instead of entering a PIN number. In the first four weeks, 10,000 customers enrolled; in a year, this number increased to 400,000 customers[107] by 2012 using this system to confirm their identity.

The Bank of New Zealand, National Australia Bank, Centrelink, St. George Bank and the Ministry of Social Development (MSD)[108] are implementing Voice ID in their contact centres, as well as other biometric systems for banking transactions. However, information security policies and compliance statutes have undergone considerable changes both locally and internationally over the last few years[109].

Given the proliferation of this type of identity verification systems and the fight against fraud and identity theft, the New Zealand parliament has passed the *Identity Information Confirmation Act 2012*[110] and *Electronic Identity Verification Act 2012*[111]. Under these Acts, the New Zealand Privacy Commissioner may call for periodic reports on confirmation service operations. While the *Identity Information Confirmation Act 2012* will help with face-to-face transactions, the current *Electronic Identity Verification Act 2012* and the identity verification service play a complementary role in the online environment[112]. This legal framework also covers

[104] http://www.salmat.com.au/products-services/speech-recognition-voice-biometrics/ (19/12/2012)
[105] New Zealand's Inland Revenue is the Tax Department http://www.ird.govt.nz/ (19/12/2012)
[106] http://www.salmat.com.au/news-insights/ (19/12/2012)
[107] New Zealand Government, Inland Revenue, *Annual Report* (2012) http://www.ird.govt.nz/resources/1/4/14a3ef004d1a9cf8915793d981e6622f/annual-report-2012.pdf (19/12/2012)
[108] http://www.msd.govt.nz/ (19/12/2012)
[109] Hunter, L., Orr, A. and White, B., "Towards a framework for promoting financial stability", (Paper presented at The Institution of Professional Engineers New Zealand, Wellington, 22 March 2006).
[110] *Identity Information Confirmation Act 2012* (NZ) in force 2013
[111] *Electronic Identity Verification Act 2012* (NZ) in force 2013
[112] (7 February 2012) 677 NZPD 138.

the RealMe program[113], which includes a combination of authentication techniques and support for biometric voice recognition system.

The New Zealand Privacy Commissioner has made two recommendations to address the adequate level of privacy protection. The first related to a proposal to amend an electronic identity credential and the second dealt with protection from liability[114].

3.6.4. *Spain: Compulsory National ID Card.* Spanish compulsory national ID cards – called DNIs- are provided by the Royal Spanish Mint (known by its acronym FNMT-RCM), which use embedded microprocessors provided by ST Microelectronics[115].

The DNI has been used for over 50 years and Spaniards over the age of 14 must present it as proof of identity for a very wide range of transactions[116]. It is governed by two laws: *Royal Decree 1553/2005 of 23 December 2005*, which regulates the issue of national identity and electronic signature certificates[117], and *Law 59/2003 of 19 December 2003*, which deals with electronic signatures[118].

The Spanish Data Protection Agency[119] has specific regulations for personal information management, namely the *Organic Law on the Protection of Personal*

[113] Clarke, Mick and Sorensen Steffen, "REALME, Technology Solution Overview" (2012) http://kantarainitiative.org/confluence/download/attachments/45059378/NZ+RealMe+Solution+Overview+v1.pdf (19/12/2012)
[114] New Zealand Privacy Commissioner "Submission to the Government Administration Committee on the Electronic Identity Verification Bill".
[115] http://www.st.com/internet/com/home/home.jsp (19/12/2012)
[116] Dirección General de la Policía y Guardia Civil, *DNI Electrónico Guía de Referencia Básica*, Comisión Técnica de Apoyo a la Implementación del DNI Electrónico (2010) [Basic eID Digital Guide] (Spain) http://www.dnielectronico.es/Guia_Basica/index.html (19/12/2012)
[117] *Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica,* BOE-A-2005-21163 [Royal Decree 1553/2005 of 23 December 2005, regulating the issue of national identity and electronic signature certificates] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-2005-21163 (19/12/2012)
[118] *Ley 59/2003, de 19 de diciembre, de firma electrónica*, BOE-A-2003-23399 [Law 59/2003 of 19 December 2003, on electronic signatures] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399 (19/12/2012)
[119] Spain, Data Protection Spanish Agency http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (19/12/2012)

Data[120] on the one hand and the *Organic Law on Exact Nature of Security Measures to Protect Personal Information*[121] on the other.

The information shown on the front of this card consists of the individual's full name, place of birth, gender, nationality, DNI number in relation to his or her tax number, photograph and signature. The information shown on the back consists of place of birth, local state or province, parents' names, address and province address. A microchip contains the individual's data, electronic photograph, signature and biometric fingerprint.

In 2008, the Spanish Minister of the Interior decided to expand the information contained in the microchip with biometric photographs and fingerprints. This proposal also included RH blood group information. However, the Spanish Data Protection Agency objected to the project, arguing that "a document that incorporates additional data would be different from electronic DNI, which would require new legislation for its implementation and development"[122]. The DNI is only used as proof of identity when Spaniards use electronic signatures for secure personal information transmitted through electronic identification systems (eID).

3.7. Conclusions

These four countries examples provide an outline of the current practices within the biometric industry. These examples also show, on the one hand the interaction between society and government, and on the other, the interaction between society and technology. There has been little debate which "underlines the deeply contested character of the transition to the tightly interdependent, knowledge-dominated, high-

[120] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, BOE-A-1999-23750 [Organic Law 15/1999 of 13 December 1999, on the Protection of Personal Data] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 (21/12/2012)

[121] *Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana*, BOE-A-1992-4252 [Organic Law 1/1992 of 21 February 1992, on the Protection of Public Safety] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-1992-4252 (19/12/2012)

[122] Europa Press, "Protección de Datos estará 'especialmente atenta' a la posible incorporación de datos nuevos en el DNI electrónico" (Media Release, 1 December 2005) http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2005/common/Interbusca.1_de_diciembre_de_2005.pdf (19/12/2012)

tech economies of the twenty-first century"[123]. The sketch of the types of political and public debates surrounding the deployment of biometric systems in the four countries support that view.

This chapter has explored the biometric industry, as well as its key players, practices, commitments and regulation. This thesis does not propose to regulate the biometric technology itself, but it does acknowledge the importance of regulating the people who will apply the technology. This chapter provides an overview of the products that have been developed by this technology. Products, such as ePassports, have not only enhanced border controls, but also play a key role in the world economy by ensuring trade with legitimate travellers. At the same time, concerns about terrorism, cross-border crimes and illegal immigrants are incentivizing national governments to adopt biometric ePassports, but this development has been with relatively little public knowledge of the biometric industry without a public debate.

The biometric industry debate should not be viewed solely in terms of a map the key players, such as IBM, HP, Microsoft, Datacard Group, Safran Morpho, Steria, Gemalto and Thales internationally. The biometric industry should be seen in terms of how this industry interacts with governments[124]. From a government's perspective, this interaction may not only leads to a potential loss of national control resulting from TBIF on international networks and platforms, but it also has an impact on national policies without public scrutiny, particularly in the context of immigration control[125] and crime prevention[126].

This chapter has also discussed some aspects of the biometric industry at the national level, because of different practices in different countries, such as Australia, Mexico, New Zealand and Spain. This thesis focuses on the individual privacy

[123] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9, p. 4.
[124] For further details, see section 1.6. The Significance of this Study
[125] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[126] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

implications rather than other legal implications related to this expanding biometric technology. In competition law, for example, it is important for the ICT legal and regulatory framework to generate conditions to promote public interest, confidence and participation in the sector. In media law, it is important to set media content regulation, spectrum regulation or net neutrality. The same happens in commerce law in terms of intellectual property and other legal fields[127].

Finally, this chapter argues for an improvement both in national level regulation and self-regulation within the biometric industry. These two levels of national regulation and industry self-regulation need to be consistent nationally and internationally but also need to be transparent and accountable.

[127] However, they are not been examined in this thesis. For further details, see section 1.5. The Aim of Research

CHAPTER 4.

BIOMETRIC SYSTEMS IN THE CONTEXT OF TRANSBORDER IMMIGRATION FLOW

4.1. Biometrics in Immigration: Information Flow

The central focus of this thesis is Transborder Biometric Information Flows (TBIF). This chapter considers the specific contexts of transborder biometric immigration information flow. A comparative study of four countries, two from the Civil Law tradition and two from the Common Law tradition[1], have been selected, as an analytic tool to identify some of the more important problems, limitations and challenges related to TBIF in the context of immigration information flow.

This chapter provides an insight of the interaction between the current deployment of biometric systems as mechanism to enhance border control and the actual way in which four countries collect, store, process and exchange immigration information flow. The chapter discusses the lack of public debate in the deployment of biometric systems and TBIF in the context of immigration information flow. The research reveals the actual mode of data collected, retrieved, analysed, stored and exchanged in the four countries examined, while highlights the technical international and national immigration policies. Finally, this chapter calls for a transparent, accountable and supervised TBIF framework in the context of immigration control.

The TBIF comparative study of immigration information flow in the four countries demonstrates that, in the absence of both specific international treaties on biometrics deployment and a self-regulating biometric industry, two international organisations have emerged and are setting significant and influential standards on the deployment of biometric systems in immigration. The International Civil Aviation Organisation (ICAO) and the International Organization of Migration (IOM) have made recommendations and established mandatory specifications in this area. In addition, two regional organisations are moving towards establishing not only

[1] For further details, see section 1.3. Country Profiles for the Comparative Study Component

recommendations and specifications, but also biometric system standards on border control strategies. These are the European Union (EU) and the Asia Pacific Economic Cooperation (APEC).

The work and publications of these organisations focus on technical aspects. Arguably, these technical aspects have not included public discussion of the social and theoretical requirements and dimensions of public debate, transparency and scrutiny[2]. Jasanoff has addressed this view in stating that "the pinpoint here are consequences for the day-to-day conduct of society, occur within elites, in the courts, the expert bodies that advice parliaments and presidents, and the professional classes that control much of the meaning making in advanced industrial societies. These are the groups, then, that can be observed enacting and performing some of the continuities of culture, with significant implications for convergence and divergence across national polities"[3].

The TBIF comparative study of the four countries, in immigration information flow, reveals two types of asymmetries. The first asymmetry relates to differences between the information collected, stored, processed, retrieved, updated, analysed and exchanged by the four countries. The second asymmetry relates to specific immigration differences in border control strategies and travel documents. For example, in the case of Mexico, biometric passports have been more recently issued for citizens, than in the other three countries. These asymmetries pose short and long-term challenges for international cooperation, an aspect that will be formally discussed further in this thesis[4].

The deployment of biometric systems in the context of immigration has been mainly to increases efficiency along national borders in the processing of immigrants generally. These measures have been adopted to enhance border security with new methods to collect and record traveller identities through with border control

[2] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States*, (Princeton University Press, 2007); Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Einaudi, 1980).
[3] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 2, p. 29.
[4] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

checkpoints. These measures also aim to stop illegal immigration, help fight cross-border crimes and prevent terrorism.

These are commendable public policy and protection goals but not such as to avoid an informed public debate on the deployment of this technology in the immigration context[5]. This chapter discusses the lack of public debates in the deployment of biometric systems and TBIF in the context of immigration information flow. The implementation of these new biometric identification systems raises legal, political and ethical concerns. The legal concerns should be tested by the principle of proportionality, discussed in a later chapter[6].

This chapter examines the interaction between the current deployment of biometric systems as mechanisms to enhance the goal of border control and the actual ways in which the four countries collect, store retrieve, analyse and exchange immigration information flow. The chapter examines this interaction in the context of developing international and national immigration policies. This chapter also examines TBIF[7] whether privacy and data protection legal frameworks are operating effectively. Finally, this chapter assesses the requirement for transparent, accountable and supervised national and international TBIF frameworks in the context of immigration control.

4.2. Transborder Biometric Information Flows: The Need for Public Debate

The deployment of biometric systems in immigration has intensified and diversified[8], however, there is a very little public discussion about this development outside of the industry and the small group of public officials working in this area. “Popular media and official discourse are the two main sources how people create and use

[5] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States*, above n 2; Habermas, Jürgen, “Sfera pubblica (Una voce di enciclopedia)”, above n 2.
[6] For further details, see section 7.4. The Principle of Proportionality: Legitimate Restrictions to Privacy and Data Protection
[7] For further details see section 1.5. The Aim of Research
[8] For further details, see section 3.3. Biometric Systems Applications: Diversification into Different Fields

"knowledge" for everyday life"[9] but there is equally little knowledge within societies about these systems and their impact on privacy and civil liberties[10].

The dynamics of the interaction between popular media and official discourse follows an important aspect of political behaviour in the implementation of biometric systems. This thesis shares Vega's argument about the free shaping of public opinion and the democratic State being closely related concepts[11]. Even more so in cases, in which biometric travel documents present legal, political and ethical concerns, mainly because these biometric documents can breach privacy and data protection rights[12].

The actual national immigration policy context in the each of the four countries study demonstrates that the decision-making processes are dominated not only by domestic concerns, but also by international security interests in preventing illegal immigration, cross-border crimes and the prevention of terrorism.

There has been a lack of multidisciplinary research on biometric surveillance systems and their technical aspects. There has also been an absence of public discussion focusing on the risks of centralised biometric databases for immigration purposes, the link between immigration information flow and information flow in criminal databases and the TBIF between countries and international organisations

[9] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States*, above n 2; Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 2.

[10] Interview with Ernesto Villanueva Villanueva and Issa Luna Pla, Professors, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [Legal Research Centre of the National Autonomous University of Mexico] (Mexico City, 23 November 2011); Interview with Charlotte Epstein, Professor, University of Sydney (Sydney, 28 October 2011); Interview with Katina Michael, Associate Professor, University of Wollongong (Sydney, 21 February 2012) This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[11] Public opinion has been Pedro de Vega's permanent area of study, which has been captured in several publications. Vega García, Pedro de, "El principio de publicidad parlamentaria y su proyección constitucional" (1985) 43 *Revista de Estudios Políticos* 45-66; Vega García, Pedro de "Significado constitucional de la representación política" (1985) 44 *Revista de Estudios Políticos* 53-74.

[12] For further details on the legal impact of biometrics, see section 2.4. Biometric Systems: Privacy Review

generates concerns. These concerns should be publicly debate in the interest of transparency and scrutiny[13].

Following the lines of argument of Jasanoff, people should be allowed to "own" their biometric characteristics once border protection personnel have extracted them for identification and verification identity purposes[14]. Sartori considers that "in a direct democracy a simple citizen must –should- know the issues over which he decides, as well as be competent, in a certain way, on the topics assigned to his competence"[15]. Citizens should be aware that they may exercise rights of access, rectification[16], challenges to the processing[17] of their biometric personal data under privacy and data protection laws. More generally, individuals need to exercise their democratic rights to request transparency and accountability in the management of biometric databases for immigration purposes and the way TBIF is carried out by countries and international organisations. This includes the democratic right to know which national and international entities are involved in the processing of biometric data and cross-border exchanges.

The principle of transparency has permeated beyond the idea of mere publicity of acts of State organizations. "Transparency" extends to ideas of State authorities' obligations to carry out their actions, as a general rule, according to prescribed powers that are publicly available. This is a major procedural mechanism to control the power and democratic legitimacy of public institutions[18]. In this case, national governments should publicly debated or provide information regarding policies on the implementation and deployment of biometric systems.

---

[13] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States*, above n 2.
[14] Ibidem, p. 27.
[15] Sartori, Giovanni, *Homo Videns, la sociedad teledirigida,* (Taurus, 2004), p. 163.
[16] In Mexico and Spain the control over personal data is exercised by ARCO or Habeas Data rights, which give the individuals to protect effectively their personal information and control over it. This ARCO rights are: Access, Rectification, Cancellation and Objection. Kuschewsky, Monika (ed.), *Data Protection and Privacy Jurisdictional Comparison* (Thomson Reuters, 2012).
[17] In Mexico and Spain instead of challenge the process of personal data, individuals exercise ARCO rights, especially Cancellation and Objection. "Cancellation is individuals' right to block free of charge their personal data when it is inadequate, excessive or unnecessary or when it is stored in a period in excess of that which is established in Law whereas Objection is individuals' right to request that the processing of their personal data not be carried out". Idem.
[18] Villanueva, Ernesto, *Derecho a la Información*, (Porrua-Camara de Diputados-Universidad de Guadalajara, 2006) pp. 69-72.

This thesis generally argues for a legal framework with an adequate level of privacy and data protection, to secure civil liberties. However, this legal framework must be accompanied by greater public debate, transparency and accountability about benefits and risks on the deployment of biometric systems and TBIF. This type of information must be available to citizens in a plain language while privacy and data protection rights are promoted in a cross-border co-operation and collaboration mechanism.

4.3. Personal Data: Inconsistencies in Data Collection Internationally

On the international level, immigration policies favour the implementation of biometric systems for the benefits of cost reduction for immigration services; lessening identity fraud; improved confidence in administration; greater efficiency in border processing; as well as preventing illegal immigrants; fighting cross-border crimes; and, preventing terrorism. This section compares the ways in which Australia, Mexico, New Zealand and Spain actually classify and collect migration data. Significantly, the four countries study shows that these countries do not and cannot easily exchange immigration information among themselves for practical classification reasons rather than technical or legal reasons. The categories of data collected by each country may not be exactly the same and differs depending on the period of time because each country's updates are not contemporaneous or harmonised. For example, the websites of Australia, Mexico New Zealand and Spain on migration statistics data present a large number of migration information regarding types of visas or categories. The four countries use different terms and expressions for visas, as well as different classifications. Another inconsistency that was found was that the terms cover different periods of time between visas. The terms and expressions differ and definitions in their migration frameworks are inconsistent, vague and contradictory. However, it is a common factor in the four countries to exclude citizens departing with the status of military personnel and their dependants and nomads, persons without a fixed place of residence who move from one site to another, are also excluded from their migration statistics.

For this reason, comparative statistical information on immigration information flow in the four countries examined is more difficult to provide in an integrated manner. Accordingly, it is possible to achieve the data collection goal of the Global Commission on International Migration (GCIM) as reported to the United Nations in 2005: "that the data collection, composition, categorisation, retrieval, collation and exchange reflect national legislative, administrative and policy imperatives"[19]. However, it is considerably more difficult to present this data in a consistent and uniform international manner.

The Organisation for Economic Cooperation and Development (OECD) and the International Organization for Migration (IOM) provide datasets, however, IOM does not have global coverage for all migration data[20] and the migration statistics collected by the OECD in many of the countries covers economic, population and labour immigration data rather than specific categories of immigration[21]. In 1998, the *Glossary to the UN Recommendations on Statistics of International Migration* was published[22]. The Glossary is a useful study about the collection of international migration statistics –including terminology and definitions- with the aim of broadly assisting the understanding of the importance of the dynamics of international

[19] This GCIM closed in 2005. Global Commission on International Migration (2005), http://www.migrationdevelopment.org/fileadmin/data/resources/gender/research_papers/GMP_No_01.pdf (20/12/2012)

[20] IOM collects and collates some regional data considered important to its operations, such as from the Commonwealth Independent States (CIS) and Statistical Information System on Migrations in Central America (SIEMCA), to obtain some of its data. IOM also sources data back to the OECD, Eurostat, UN Population and Statistics Division, US Census Bureau and other UN agencies known to have reliable data on the subject matter it covers. http://www.iom.int/cms/about-migration (20/12/2012)

[21] In its entry of international migration data, the OECD notes in material posted on its website under the headings "OECD Factbook 2010" and "Country Statistical Profiles 2010" that the sources of migration statistics in many of the countries it covers are population registries; residence or work permits; acceptances for permanent settlement; censuses; and, surveys. However, it observes that a wide variety of other data sources exists, such as border crossing counts, analyses of passenger landing cards and special surveys like labour force surveys. http://www.oecd-ilibrary.org/search?option1=titleAbstract&option2=&value2=&option3=&value3=&option4=&value4=&option5=&value5=&option6=&value6=&option7=&value7=&option8=&value8=&option9=&value9=&option10=&value10=&option11=&value11=&option12=&value12=&option13=&value13=&option14=&value14=&option15=&value15=&option16=&value16=&option17=&value17=&option21=discontinued&value21=true&option22=excludeKeyTableEditions&value22=true&option18=sort&value18=&form_name=quick&discontin=factbooks&value20=18147364%2C15615537&option20=factbooks&value1=country+statistical (20/12/2012)

[22] This document identifies the core and optional information for all categories of international migrants. *UN Recommendations on Statistics of International Migration*, UN Department of Economic and Social Affairs Statistics Division (1998) http://unstats.un.org/unsd/publication/SeriesM/SeriesM_58rev1E.pdf (20/12/2012)

migration, its causes and effects. More recently, in 2004, IOM published its *Glossary on Migration*[23]. However, these reports do not set mandatory standards for member countries in the collection and presentation of migration data, the reports have only the status of recommendations.

There is also a problem in immigration data because of an absence of universally accepted definitions in this area. The absence of a precise definition for terms and the lack of international standards for data collection in immigration impede and prevent exact comparisons[24]. From 2008 to 2009, Australia and New Zealand adopted part of the *Glossary of the UN Recommendations on Statistics of International Migration*. Since that date Australia, Mexico, New Zealand and Spain have some consistent and complete series of immigration statistics flows that conform well to the definitions for long-term migration as suggested by the United Nations. Nevertheless, the definitions for short-term migration information differ in terms for categories of visas, as well as different visa's classifications terms. These countries have their own databases for foreigners who enter as temporary residents. The problem lies in their current data collection systems and the categories for short-term migration information contained in their own databases for foreigners because all four countries have not adopted completely the Glossary and there are actual inconsistent with the terminology.

Australia is able to consult its own immigration-based databases for significant information about migrants. However, data about population by country of birth, age and sex are usually taken from periodical censuses which are updated from immigration data between censuses, as well as from registers of deaths. Australian data on immigrants' employment status is taken, for example, from monthly labour surveys or from specific migrant surveys that are conducted from time to time[25]. However, historical statistics related to certain immigration categories can be found since 2002.

---

[23] Perruchoud, Richard (ed), "Glossary on Migration", *International Migration Law*, (IOM, 2004) http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/published_docs/serial_publications/Glossary_eng.pdf (20/12/2012)

[24] *UN Recommendations on Statistics of International Migration*, UN Department of Economic and Social Affairs Statistics Division (1998), above n 22.

[25] Australia Government, Department of Immigration and Citizenship, *Annual Report* (2011-2012)

As a “developed” country, Mexico has most of its data entered and recorded electronically so can be retrieved with relative ease. It has been updated regularly, on a monthly basis since 2002. Furthermore, historical statistics for specific categories have been in existence since 1995[26]. However, if a comparison between the classification of visas between Mexico and Australia were undertaken, inconsistencies would be apparent. Australia classifies its types of visas as temporary and permanent with 140 subclasses of visas while Mexico classifies them as visitor and resident with only 10 subclasses[27].

In New Zealand, there is a range of government agencies that collect data on international migration movements and their outcomes. Having different data collection and collation agencies creates challenges to exchange accurate information without considerable effort. This has led to a requirement for the development of a cross-agency view, based on each agency’s considering the “risks and benefits” for its own data collection. However, historical statistics regarding certain immigration categories can be found since 1998.

Spain has a mix of manual retrieval of hard copy records and electronic collation of data. The information collected is updated every three months. However, the numbers come from immigrants who are registered on a neighbourhood list for a particular city council (municipality) of Spain. This immigration registration is obligatory for education and academic positions and to obtain the health (sanitary) card. Historical statistics related to immigration can be found since 1996[28].

The four countries study revealed the common use of biometric passports and visas; but, again without common and consistent data collection. Australia and New Zealand collect facial and iris characteristics for their respective nationals, whereas Spain and Mexico collect facial and fingerprints characteristics for their nationals. For

[26] Mexico, National Institute of Migration (INM) historical statistics website http://www.inm.gob.mx/index.php/page/Series_Historicas (20/12/2012)
[27] For further details, see Appendix H. National Immigration Policy
[28] Spain, National Institute of Statistics (INE) http://www.ine.es/ss/Satellite?L=0&c=INEPublicacion_C&cid=1259924959454&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout&param1=PYSDetalleGratuitas (20/12/2012)

border control processing of foreign travellers these four countries use face recognition system which is used to verify traveller's identity and check blacklists. However, this is combined with the traveller's type of visa. Not all the types of visa issued by the four countries are biometric.

These asymmetries raise the question why the deployment of biometric technology in immigration control was differently applied into the four countries. Jasanoff would argue that even these differences are hard to explain, this only makes the task the more intellectually engaging[29]. Nevertheless, apart from iris and fingerprint data differences, the four countries have deployed biometric systems for immigration purposes with centralised biometric databases; their border control procedures and processing are common; biometric verification at the border control process is used to check against criminal biometric databases; and, the four countries have common control strategies deployed in immigration.

4.4. Immigration Policy: The International Context

Immigration occurs for many reasons: the search for better economic opportunities, the wish to join family members who have migrated or the escape from political conditions in a country. Article 13(2) of the *Universal Declaration of Human Rights* recognises that: "everyone has the right to leave any country, including his own and to return to his country"[30]. The international community has declared this right necessary to protect other human rights. The right to travel is a necessary attribute of a democratic constitutional State. Immigration and migration play important roles in the complex rapid and often violent process of change in the current international political order in many regions of the world. This change has impacts on States, regions, societies, economies and policies[31].

[29] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 2, p. 8 and 9.
[30] Adopted by the General Assembly of the United Nations. *Universal Declaration of Human Rights, adopted by G/A/RES 217A (III) of 10 December 1948*, article 13(2).
[31] Boudin, Leonard B., "The Constitutional Right to Travel" (1956) 56 *Columbia Law Review* 47-75.

The international legal framework composed of treaties, conventions, principles and agreements are balanced with State sovereignty rights to protect borders, to confer nationality, to admit and expel foreigners, to combat trafficking and smuggling and to safeguard national and regional security. These international legal frameworks need to be balanced not only with citizens' right to leave their country, but also with other human rights involved in immigration issues, such as privacy and data protection rights. This international legal framework of human rights constitutes the main pillars of public policies on international immigration. This thesis will test these issues and arguments by examining the balancing of private and public interests[32].

4.4.1. *The Deployment of Biometric Technology*. The deployment of biometric technology for immigration purposes must be legitimate and have a basis on constitutional grounds[33] to be justified and applied in a democratic constitutional State[34]. Thus, the "knowledge" of the technical and legal aspects of biometric systems is essential for elected officials in charge of authorizing and, implementing this type of technology into comprehensive and integrated programs[35].

"Defining policy", argues Jasanoff, "is not a sure fire recipe for placating constituents at home, as politicians in the globalizing world have discovered to their sorrow. In policy as in politics, there is no substitute for a committed domestic constituency satisfied with the handling of immediately recognizable local problems"[36].

The implementation of biometric systems give rise to controversial legal issues particularly in relation to constitutional safeguards as biometric technology directly affects individual privacy and data protection rights. This legal concern must be addressed to secure political support and public acceptance for biometrics in public

[32] For further details, see section 7.4. The Principle of Proportionality: Legitimate Restrictions on Privacy and Data Protection
[33] For further details, see section 1.4 Hypothesis
[34] It is true that every State has a Constitution, but not all of them are constitutional States. García De Enterría, Eduardo, *La Constitución como norma y el Tribunal Constitucional*, (Editorial Civitas, 2006), p. 43.
[35] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 2; Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* above n 2.
[36] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* above n 2, p. 85.

policies. The legal response to this concern must consider the balance required within the proportionality test[37].

4.4.2. *International Organisations in Immigration*. There are no specific United Nations, General Assembly international treaties or conventions issued and approved related to the implementation of biometric systems for immigration purposes. However, on an international level, Article 13 of the *Convention on International Civil Aviation* deals with the deployment of biometric technology and states:

> "The laws and regulations of a contracting State as to the admission to or departure from its territory of passengers, crew or cargo of aircraft, such as regulations relating to entry, clearance, immigration, passports, customs, and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State"[38].

The two key international organisations operate in the biometric migration area. The International Civil Aviation Organization (ICAO) is the principal international organisation for international standards, recommendations and procedures regarding immigration practices. ICAO is in charge of biometric passports and visa specifications[39]. Since 1995, ICAO has been investigating biometrics and its potential to enhance identity confirmation in travel documents. However, it was not until 2001 that a recommendation of the use of facial recognition as the primary biometric was released[40].

---

[37] For further details and the equivalent Common Law reasonableness standard, see Chapter 7. Transborder Biometric on Privacy and Data Protection: National Solutions

[38] *Convention on International Civil Aviation opened for signature 7 December 1944 (entered into force 4 April 1947),* Article 13.

[39] For further details, see section 3.3.2. ePassport Technology: The New Generation

[40] ICAO, *Selection of a Globally Interoperable Biometric for Machine Assisted Identity Confirmation with MRTDs*, Technical Report (2001) http://www.icao.int/Security/mrtd/Downloads/Technical%20Reports/ICAO_MRTD_History_of_Interoperability.pdf (27/11/2012)

Secondly, the International Organization for Migration (IOM) is the other leading international organisation for migration. The IOM offers "advice, research, technical cooperation and operational assistance to States, intergovernmental and non-governmental organizations and other stakeholders, in order to build national capacities and facilitate international, regional and bilateral cooperation on migration matters"[41].

ICAO and IOM are the two main international organisations that have made recommendations and established specifications for biometric systems to be deployed in immigration policies.

4.4.3. *International Civil Aviation Organization (ICAO).* The International Civil Aviation Organization (ICAO) is a specialized agency of the United Nations that has the responsibility of adopting international standards and recommended practices and procedures regarding immigration[42].

The *Convention on International Civil Aviation* sets the structure of ICAO[43]. The following figure shows the four countries examined as ICAO contracting members. It is important to highlight that Australia, Mexico and Spain are all Council member States[44].

ICAO has developed several standards related to travel documents, principally passports and visas, as well as for border control policies on identification. A passport is not only a certificate of identity; it is also a promise of protection, with the implication that it can be withheld if the government considers the citizen unworthy of

[41] IOM, International Organization for Migration http://www.iom.int/cms/en/sites/iom/home/about-iom-1/mission.html (20/12/2012)
[42] http://www.icao.int/Pages/icao-in-brief.aspx (20/12/2012) See also, Turak, Daniel C., *The Passport in International Law*, (Lexington Books, 1972), p. 30.
[43] The *Convention on International Civil Aviation* is also known as the Chicago Convention. It took place in 1944. According to the terms of the Convention, ICAO is made up of an Assembly, a Council of limited membership with various subordinate bodies and a Secretariat. The chief officers of the ICAO are the President of the Council and the Secretary General. *Convention on International Civil Aviation opened for signature 7 December 1944 (entered into force 4 April 1947)*.
[44] ICAO Council Members http://www.icao.int/MemberStates/Member%20States.English.pdf (20/12/2012)

such protection[45]. A passport[46] is evidence of the protection to which people of a nationality are entitled to receive from their government when travelling in foreign countries[47].

An ePassport issued in compliance with ICAO specifications contains biometric data to which access needs to be controlled. These specifications include a contactless microchip[48] with a data storage capacity of at least 32kb.

For ICAO, the only method of linking a person unequivocally with a document is through a physiological characteristic of that person associated with travel document in a tamper-proof manner. The biometric characteristics that ICAO[49] uses for identification in ePassports[50] are: a) facial recognition as mandatory, and b) fingerprint or iris recognition as optional.

ICAO chose facial identification as mandatory for recognition in biometric passports because face photographs are considered non-intrusive for biometric data verification. Face photographs can be used by a person or automated face recognition systems, either for confirmation of claimed identity (recognition) by searching a database of face images for determining the authentication (verification) of the image[51].

[45] Turak, Daniel C., *The Passport in International Law,* above n 42.
[46] The standard states that "a valid passport shall be the basic document providing public authorities with information relating to the individual passenger on arrival or departure of a ship". Ibidem, p. 31.
[47] Boudin, Leonard B., "The Constitutional Right to Travel", above n 31; Turak, Daniel C., *The Passport in International Law*, above n 42.
[48] ICAO, "Why ICAO Selected the Face as Primary Biometric Identifier specified to ePassports", *MRTD Report* (2007) http://www2.icao.int/en/MRTD2/ReportsPastIssues/ICAO%20MRTD%20Report%20Vol.%202%20No.%201,%202007.pdf (20/12/2012)
[49] ICAO *Machine Readable Travel Documents, DOC 9303,* (Pt 1, 6th ed, 2006) vol. 2 http://www.icao.int/publications/Documents/9303_p1_v2_cons_en.pdf (20/12/2012)
[50] For further details, see section 3.3.2. ePassport Technology: The New Generation
[51] Face photographs are used in passports, visas, driver licences or other identification documents. ICAO, "Why ICAO Selected the Face as Primary Biometric Identifier specified to ePassports", above n 48.

The optional biometric fingerprint or iris characteristics are also available for recognition purposes. These options can be used when States may have existing fingerprint or iris databases in place against which they can verify these biometric characteristics.

4.4.4. *International Organization for Migration (IOM*). The International Organization for Migration (IOM) was created in 1951 and specialises in the field of migration and works closely with governmental, intergovernmental and non-governmental partners[52]. IOM, partnered with ICAO and the company International Business Machine (IBM)[53], is increasingly being called upon to assist States to address complex border management issues[54].

> "In support of IOM strategy, IBM activities are directed at helping governments create policy, legislation, administrative structures, operational systems and the human resource base necessary to respond effectively to diverse migration challenges and to institute appropriate migration governance. Such activities are designed as partnerships, with the requesting government and other relevant interlocutors working closely with the IBM Team to identify needs, determine priority areas, and shape and deliver interventions.
>
> The IBM portfolio is steadily growing, with over 300 active projects valued at nearly USD 90 million implemented worldwide in 2010"[55].

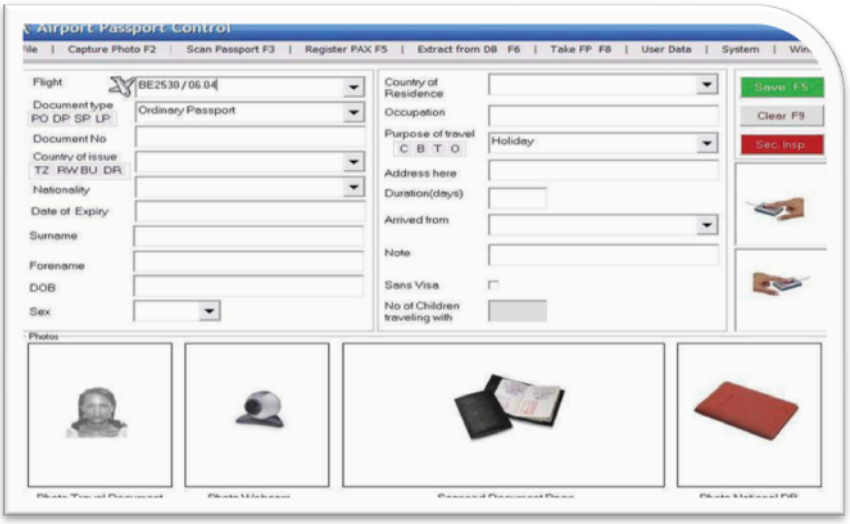
IOM works with States to assess and improve the integrity of their travel and identity documents. IOM, along with ICAO and the company IBM, have a programme for "Identity Management"[56]. IOM's Identity Management program covers two main

[52] IOM, International Organization for Migration http://www.iom.int/cms/about-iom (20/12/2012)
[53] This company was identified in Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships
[54] http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/01-IOM-IBM-FACT-SHEET-IBM-Programme-general-overview.pdf (20/12/2012)
[55] Idem.
[56] http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/06-IOM-IBM-FACT-SHEET-Identity-management.pdf (20/12/2012)

areas: a) travel documents and related issuance systems and b) travel document inspection[57].

As part of this Identity Management program, IOM also has a Personal Identification and Registration System (PIRS), which allows the collection, processing and storage of traveller information, including biometric data[58]. The PIRS can also be linked to Interpol's I-24/7 Global Communication System for Interpol's Lost Travel Documents Database[59]. The following figure shows the PIRS screen.

Figure 11. Personal Identification and Regulation System (PIRS) [60]



As part of the Immigration and Border Management program, IOM operates the Immigration and Visa Support Solution project (IVSS)[61]. IVSS includes: "1) country information; 2) logistical assistance to support visa processing; 3) skills and language testing facilitation; 4) visa application assistance; 5) travel document handling; 6) visa application centres; 7) interview facilitation; 8) self-payer health assessments; 9) DNA services; 10) biometrics enrolment; 11) document integrity and

[57] Idem
[58] http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/08-IOM-IBM-FACT-SHEET-Border-Migration-Information-System-BMIS.pdf (20/12/2012)
[59] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow
[60] Image obtained from the following source http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/09-IOM-IBM-FACT-SHEET-Personal-Identification-and-Registration-System-PIRS.pdf (20/12/2012)
[61] http://www.iom.int/jahia/webdav/shared/shared/mainsite/activities/ibm/11-IOM-IBM-FACT-SHEET-Immigration-and-Visa-Support-Solutions-IVSS.pdf (20/12/2012)

verification; 12) self-payer travel assistance; 13) web-based visa appointment scheduling and visa issuance systems; 14) border management information systems; 15) information services and 16) family tracing"[62].

4.4.5. *Global Interoperability Challenges*. For all biometric systems, the enrolment, data processing, personalisation, issuance, storage, lecture and verification of an image are necessary to achieve global interoperability. However, there are three classes of fingerprint biometric systems: finger image-based systems, finger minutiae-based systems and finger pattern-based systems[63]. Systems for iris biometrics emerged based on the methodology of one ICAO-recognized technology vendor[64].

In the short-term, these different types of biometric fingerprint systems do not present any challenge because the biometric information stored on ePassports are matched against the information stored on a country's own databases on the arrival of its own citizens. However, in the long-term, these dissimilar types of biometric fingerprint systems may present challenges to global interoperability.

There are other long-term challenges posed by many factors that can affect the performance of face recognition, fingerprints and iris recognition systems:

a) An individual's appearance, such as his or her facial characteristic, hair style, and accessories; and the image acquisition conditions, such as the camera's field of view, focus and shutter speed, depth of field, background and lighting[65]. Many countries are issuing biometric passports[66] under their own guidelines for

[62] Idem.
[63] Early on, the systems were not interoperable and as a result, there are three systems for fingerprint interoperability: image data storage, minutiae data storage and pattern data storage.
[64] ICAO, "Why ICAO Selected the Face as Primary Biometric Identifier specified to ePassports", above n 48.
[65] Face Image Data was approved as an international standard by ISO/IECJTC1 SC37 in 2005. This standard defines a data format for digital face images to allow interoperability among face image processing systems.
[66] For further details, see section 3.3.2. ePassport Technology: The New Generation.

producing and submitting face photographs following ICAO requirements[67]: this is the case with Australia[68], Mexico[69], New Zealand[70] and Spain[71]. In this respect ICAO's illustrative guidelines for Machine Readable Travel Document (MRTD) were updated in October 2013[72].

b) Image quality factors such as resolution, contrast and brightness, as well as other factors, affect the accuracy of face and iris recognition, including subject positioning, pose and expression, illumination uniformity, and, in the case of faces, the use of eyeglasses or makeup, as well as the time difference between two photographs being compared, for instance[73]. However, in the case of iris recognition is considered intrusive. During the enrolment process, an expert can determine whether the person suffers from common medical conditions like diabetes, arteriosclerosis or hypertension. The system can produce a false acceptance, false match or false rejection for a person whose iris has already been recorded but has been diagnosed with glaucoma[74].

c) Fingerprints can also be inexact. A person who handles chemical products could present a false rejection in fingerprint biometrics because these chemicals can cause a reduction of a fingerprint quality over time. Other inexact fingerprint individuals are the elderly and children under the age of six.

[67] ICAO has consequently designed illustrative guidelines for portraits in a Machine Readable Travel Document (MRTD) for the next generation of electronic passports, the so-called biometric Passports. *ICAO Machine Readable Travel Documents,* above n 49.
[68] Australia photo guidelines https://www.passports.gov.au/images/photo_guidelines.pdf#zoom=100 (20/12/2012)
[69] Mexico photo guidelines http://www.sre.gob.mx/index.php/primera-vez/252 (20/12/2012)
[70] New Zealand photo guidelines http://www.passports.govt.nz/Passport-photos---adults (20/12/2012)
[71] Spain photo guidelines http://www.interior.gob.es/pasaporte-29/clases-y-requisitos-183?locale=es (20/12/2012)
[72] For further details, see section 3.3.2. ePassport Technology: The New Generation
[73] ISO/IEC 19794-5:2005, Information Technology –Biometric Data Interchange Formats –Part 5: Face Image Data- AMENDMENT 1: conditions for taking photographs for face image data (2007). The International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 19794-5 Biometric Data Interchange Formats defines a standard data format for digital face images to allow interoperability among face recognition systems, government agencies, and other creators and users of face images.
[74] Van Der Ploeg, Irma, "Biometrics and Privacy: A note on the politics of theorizing technology" (2003) 6 *Information, Communication & Society* 85-104.

In 2004, an open letter on the dangers of biometric passports was sent to ICAO by the Non-Government Organization (NGO) Privacy International and signed by many other NGOs from around the world. In this letter, the NGOs expressed their concerns regarding the disproportionate effects of the implementation of biometric travel documents on privacy and civil liberties. They expressed their greatest concern over the creation of centralised national biometric databases[75].

4.4.5. *Regional Organisations*. Apart from the two key international organisations of ICAO and IOM, there are some important regional organisations implementing biometric systems for immigration purposes. The European Union (EU) and the Asia Pacific Economic Cooperation (APEC) are significant standard setting organisations at the regional level.

Uniform immigration policies on a global basis may be unachievable because of the wide range of immigration issues related to countries' interests around the world. However, the harmonisation of policies on regional bases is becoming more common. For example, within the European context, the Schengen Information System (SIS) and EURODAC system[76] are promoting a common visa policy under which a visa is valid in any Schengen-zone country[77] and may be issued by one country for travel to another. In the Asia Pacific context, the APEC has created a Business Travel Card (ABTC) that facilitates short-term entry to participating member countries (referred to as member 'economies')[78]. These common regional visa policies have developed because of the confluence of interests in these countries have in the movement of migrants through their regions.

[75] "Privacy International was founded in 1990 and was the first organization to campaign at an international level privacy issues". Gus Hosein, *Privacy International was founded in 1990 and was the first organization to campaign at an international level privacy issues* (30 March 2004) Privacy International https://www.privacyinternational.org/blog/open-letter-to-un-agency-on-dangers-of-biometric-passport-standard (20/12/2012)

[76] For further details, see Appendix E. Eurodac Introductory Information

[77] The Schengen zone includes 26 countries: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Slovenia, Slovakia, Spain, Sweden, and Switzerland. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm (20/12/2012)

[78] http://www.apec.org/About-Us/About-APEC/Business-Resources/APEC-Business-Travel-Card.aspx (20/12/2012)

As far as the EU is concerned, "[i]nternational terrorism is, because of its cross border dimensions, a migration issue. But immigration policy, particularly on border control, is just one area where national and international enforcement measures can be taken against terrorism"[79].

The reach of these regional organisations extends to interactions between the four countries study group of Australia, Mexico, New Zealand and Spain. Australia, Mexico and New Zealand are country members in APEC these three countries interact with the EU and Spain is member of the EU. These interaction are significant when migration data is exchanged with these regional organisations.

4.4.6. *Introduction of Biometric Systems: Regional Organisations*. In the four countries study three main biometric systems were identified, two in Europe and one in Asia-Pacific. The following three examples of biometric systems for biometric travel documents discussed below. Also includes standards for interoperability, security and accuracy designed by ICAO.

In 2009 at the APEC Business Mobility Group, Australia submitted as part of the Proposed Business Mobility Group Goals for 2009 that: "[t]he document 'A guide to Biometric Technology in Machine Readable Travel Documents' has already been recognized as a unique and valuable document by ICAO and the ISO, and also by the IOM, which now has permission from APEC to translate the document into the other languages to assist other governments adopt e-Passports"[80]. The following three examples of the biometric systems in the deployment and the process of collection and storage of biometric information.

- *EURODAC system*[81]: In 2000, the EURODAC system was established and linked to the "Dublin Convention" to establish a centralized European database on asylum seekers and other non-European Union nationals

[79] Van Krieken, Peter J. (ed), *Terrorism and the International Legal Order, With special Reference to the UN, the EU and Cross-Border Aspects*, (T.M.C. Asser Press, 2002), p. 441.
[80] Australia Government "Consideration to the Asia Pacific Economic Cooperation (APEC) on the Proposed Business Mobility Goals for 2009".
[81] For further details, see Appendix E. Eurodac Introductory Information

apprehended while illegally crossing borders into EU territory. It includes fingerprints[82].

EURODAC Automated Fingerprint Identification System (AFIS) was created by the company Steria[83]. Each Member State has national access points and works directly with individuals national administrations. The fingerprints taken are compared with the fingerprint data transmitted by other Member States already stored in the central database. If the EURODAC System detects that fingerprints have been already collected and stored the asylum seeker is redirected to the Member State where his/her fingerprints were originally collected and stored.

- *Schengen Information System[84] (SIS II)*: For the operation of the border control free system among the Schengen member States, the SIS II provides the main support system. It contains a "list" of people who have committed an offence, are missing or are under observation.

Member States feed the system with information through national networks which are connected to a central system and supplemented by the SIRENE network[85] made up of representatives from the national and local police, customs agencies and the judiciary[86]. This system was reviewed after the "Prüm Convention"[87]. The company Steria is leading the second generation of the Schengen Information System (SIS II)[88]. Its capacity was increased not only technologically, but also in relation to the information collected, stored and exchanged.

---

[82] Idem.
[83] This company was identified in Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships http://www.steria.com/sharing-our-views/success-stories/?cr_uid=185 (20/12/2012)
[84] For further details, see Appendix F. Schengen Information System
[85] SIRENE network is a system used by police authorities to exchange information in compliance with the Schengen Convention for the purposes of preventing and detecting criminal offences in Schengen zone by SIS II. For further details, see Appendix F. Schengen Information System
[86] International Organization for Migration, "International Terrorism and Migration", *Background Paper*, Immigration and National Security, (2003), 16 http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/activities/tcm/Int_terrorism_migration.pdf (20/12/2012)
[87] For further details, see Appendix G. Prüm Convention
[88] This company was identified in Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships. Steria, "Steria successfully launches the second generation Schengen Information System for the European Commission (SIS II)" (Media Release, 8 July 2013)

- *APEC Business Travel Card (ABTC):* Using agreed regulations this card exchanges information through an online system in order to enhance the mobility of business people in the region. It contributes information on lost and stolen travel documents to the International Criminal and Police Organisation (ICPO-INTERPOL) database[89].

Member countries are in charge of issuing the Business Travel Card complying card eligibility criteria; service standards; and, card manufacturer standards[90]. It eliminates the application for visas when visiting APEC members. However, passports remain as the primary travel document. TBIF includes: requesting clearance in advance; receiving clearance; and, requesting card production. The TBIF is encrypted during transfer via a centralised database.

In summary, regional organisations have been not only deploying centralised biometric systems, but also encouraging TBIF for immigration control. These three regional biometric systems are using ICAO's and APEC's technical security standards. However, the fact that these regional biometric systems are centralised databases poses a common question about technological vulnerability and privacy risks regarding the unauthorised access, hackers and back-ups. These privacy and data protection concerns are further discussed[91]. In addition, it is interesting to note that the same company, Steria was in charge of the two major biometric systems in Europe.

---

http://www.steria.com/media/press-releases/press-releases/article/steria-successfully-launches-the-second-generation-schengen-information-system-for-the-european-comm/ (11/09/2013)

[89] http://www.businessmobility.org/travel/index.asp (20/12/2012)

[90] APEC *Guiding Principles for PKI-Based Approaches to Electronic Authentication* (2005) http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel/annex_d.aspx (20/12/2012)

[91] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

4.5. Immigration Policy Framework and Systems in the Four Countries Study

The contexts of immigration information was included in the four countries study and immigration policy in Australia, Mexico, New Zealand and Spain was analysed. The results identified the legal problems, limitations and challenges in TBIF. In Chapter 7 the legal problems, limitations and challenges are assessed for a proportional and harmonised legal framework in TBIF[92].

Mexico has two authorities, in one hand the Ministry of Interior through the National Institute of Migration (INM)[93] managing arrivals; departures; and, settlement of migrants, and in the other the Ministry of International Affairs is in charge of managing passports issuing and protect Mexican human rights overseas. Spain has also two specific authorities[94] managing arrivals, departures and settlement of migrants, this can be a result of being both Civil Law countries. However, there is a main difference between Mexico and Spain. In Mexico, the Ministry of Interior as many other federal countries is responsible for the general interior security of the country; these could be seen rare, but Mexico has some of the most complex immigration dynamics in the world[95]. Nevertheless, a distinguished characteristic between the two Common Law countries is that in New Zealand four authorities are involved in immigration[96] whereas in Australia[97] only one.

[92] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

[93] Mexico, National Institute of Migration (INM) http://www.inm.gob.mx/index.php/page/pagina_principal/en.html (20/12/2012) For further details, see see Appendix H. National Immigration Policy

[94] Spain, General Minister for Migration and Immigration http://extranjeros.mtin.es/es/Organizacion/ (20/12/2012) For further details, see see Appendix H. National Immigration Policy

[95] The flow of undocumented people from Mexico, Central and South America across the northern border to the United States continues while Mexico's southern border is increasingly used by citizens from Central and South America as their way into the United States. "Some 200,000 Central Americans attempt to irregularly enter the US via Mexico's southern border. Although 70 per cent of them are detained by Mexican migration authorities and returned to their countries of origin, an estimated 60,000–70,000 eventually reach the US or remain in Mexico". IOM, *Migration Initiatives Appeal 2010* (2010) http://publications.iom.int/bookstore/free/Migration_Initiatives_2010.pdf (20/12/2012)

[96] New Zealand immigration area of responsibility http://www.dol.govt.nz/about/responsibilities/ (22/12/2012) For further details, see see Appendix H. National Immigration Policy

[97] The Department of Immigration and Citizenship (DIAC) http://www.immi.gov.au/ (20/12/2012)

The following figure shows the four countries immigration policy, for a complete description on the four countries immigration policy see Appendix H[98].

Figure 12. Immigration Policy

	Australia	Mexico	New Zealand	Spain
Authority	DIAC	Ministry of Interior, National Institute of Migration (INM) and Ministry of International Affairs	Department of Labour, Department of Internal Affairs (Citizenship Branch), Electoral Enrolment Centre and Department of Internal Affairs (Births, Deaths and Marriages)	Minister of Labour and Migration by the Secretary of Migration and Immigration
Legislation	*Migration Act 1995*	*Migration Law* *General Population Law* *Refugees and Complementary Protection Law*	*Immigration Act 2009*	*The 2/2009 Organic Law* *Royal Decree 1161/2009*
Reforms/Amendments	yes	yes	No	yes
Immigration Policy (collection and process of biometrics)	yes	yes	yes	yes
Biometric passports	yes	yes	yes	yes
Biometric visas	yes	yes	yes	yes
Other control strategies deployed	yes	yes	yes	yes

Source: Legislation of the four countries study, *Migration Act 1995* (Australia), *Migration Law, General Population Law, Refugees and Complementary Protection Law* (Mexico), Immigration Act 2009 (New Zealand), *The 2/2009 Organic Law and Royal Decree 1161/2009* (Spain)

The immigration policy and legal framework in each country differs. Both Australia and New Zealand as Common Law countries have just one law[99] dealing with immigration, whereas Mexico[100] and Spain[101] as Civil Law countries have more than

[98] For further details, see Appendix H. National Immigration Policy

[99] *Migration Act 1995* (Cth) and *Immigration Act 2009* (New Zealand)

[100] *Ley de Migración, DOF 25/052011 [Migration Law] (Mexico)* http://www.diputados.gob.mx/LeyesBiblio/pdf/LMigra.pdf *(20/12/2012); Ley General de Población, DOF 07/01/1974 [General Population Law, last amendment 09/04/12] (Mexico)* http://www.diputados.gob.mx/LeyesBiblio/pdf/140.pdf *(20/12/2012)* and *Ley sobre Refugiados y Protección Complementaria, DOF 27/01/2011* [Refugees and Complementary Protection Law] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LRPC.pdf (20/12/2012)

[101] *Ley Orgánica 2/2009, de 11 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social,BOE-A-2009-19949 [Organic Law 2/2009 amending Organic Law 4/200 on the Rights and Liberties for Foreigners in Spain and their Social Integration] (Spain),* http://www.boe.es/buscar/doc.php?id=BOE-A-2009-19949 *(20/12/2012)* and *Real Decreto 1161/2009, de 10 de julio, por el que se modifica el Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España de ciudadanos de los Estados miembros de la Unión Europea y de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo, BOE-A-2007-4184, [Royal Decree on the Entry, Free Movement and Residence in Spain of Citizens of the Member States of the European Union and Other States Party to the Agreement on the European Economic Area] (Spain)* http://www.boe.es/buscar/doc.php?id=BOE-A-2007-4184 *(20/12/2012)*

one piece of legislation. Nevertheless, Australia, Mexico and Spain have been active in amending or reforming their immigration framework in the recent years[102].

The four countries are active in developing their immigration policy in relation to the collection and processing of biometric information. In addition, all four countries are issuing ePassports[103], through the implementation of ePassport technology in the four countries has been different. In the case of Spain, as a member of the EU, implementation is to follow and to adopt EU decisions. Australia and New Zealand are part of the Five Nations Passport Group[104] and adopt the common consensus on ePassport technology. Mexico has been solely responsible for its immigration control strategies.

In relation to the collection of biometric information for visas, the four countries differ significantly not only in their varieties of categories of visa but also in the countries listed to apply for a visa; however, the four countries share a common criteria on the collection of biometric data in refugee cases. The following figure shows the general asymmetries relating of categories of visas.

Figure 13. Four Countries Type of Visa

Types of visa	Australia	Mexico	New Zealand	Spain
Permanent	6	3	2	2
Temporary	6	7	4	7

Source: Legislation of the four countries study, *Migration Act 1995* (Australia), *Migration Law, General Population Law, Refugees and Complementary Protection Law* (Mexico), Immigration Act 2009 (New Zealand), *The 2/2009 Organic Law and Royal Decree 1161/2009* (Spain)

[102] For further details, see Appendix H. National Immigration Policy

[103] While Australia and New Zealand are issuing biometric passports with Basic Access Control (BAC), Spain is issuing biometric passport with Supplemental Access Control (SAC). Mexico is also issuing biometric passports but it was not possible to identify what type of ePassport technology has been implemented. For further details, see section 3.3.2. ePassport Technology: The New Generation

[104] The Five Nations Passport Conference is a forum between the passport issuing authorities in Australia, Canada, New Zealand, the United Kingdom and the United States to "share best practices and discuss innovations related to the development of passport policies, products and practices" Australia Government, Department of Immigration and Citizenship, *Annual Report* (2010-2011)

An accurate and direct comparison between the terms used for categories of visa in the four countries is difficult to achieve as, the four countries used different terms. Mexico and Spain as Civil Law countries do not use same terms. Mexico uses the terms “visitors and residents”, Spain uses the terms “stays (estancias) and residence”. Australia and New Zealand, as Common Law countries, do not use the same terms. Australia uses the terms “permanent and temporary”, whereas New Zealand uses the terms “residence class and temporary entry class”[105].

Another asymmetry is the different number of categories and subcategories of visas. Australia has six categories of permanent visa and six categories for temporary visa. However, the categories of permanent and temporary visas have approximately 140 visa subclasses with their own sets of eligibility criteria. The New Zealand residence class visa has two subcategories and the temporary entry class visa has four subcategories. However, these subcategories have an additional variety of eligibility criteria. The Mexican visa category of visitors has seven categories of visa and residents’ category has three types. The Spanish category of “stays” visa has seven categories and the residence visa has two subcategories. The four countries have complex categories of visas, none of them are exactly the same.

This four countries study demonstrates a common, though not uniform, immigration policy on the deployment of biometric systems. It also demonstrates the diversity of practices, ePassport issuance and government structures in the context of immigration policy. In addition, in the four countries it was possible to identify common control strategies deployed in immigration[106].

4.5.1. *The Implementation of Biometrics in Immigration as Policy*. At the national level it was possible to identify in the four countries study, the inclusion of biometric technology as part of immigration policy. In the four countries study, the immigration policies have common objectives related to: economy, national identity, opportunity

[105] For further details, see Appendix H. National Immigration Policy.
[106] For further details, see section 4.5.3. Common Control Strategies Deployed in Immigration at the International Level

for families and national security, as well as prevention of illegal immigration, cross-border crimes and terrorism[107].

In general terms the deployment of biometric systems for immigration control is to provide an effective and efficient scrutiny at the border by examining passengers and crew and their movement information before their arrivals, departures and settlement of migrants. In addition, biometric systems provide identification and verification by matching TBIF[108]. The following figure presents the biometric systems implemented by the four countries study:

Figure 14. Biometric Systems in the Four Countries Study

Countries	Information and Biometric ID Systems
Australia	SmartGates Business Travel Card (APEC) Movement Alert List (MAL)
Mexico	Foreigners and Refugees List Business Travel Card (APEC) Consular Management Integrated System (ACIS) Integrated Migration Operations (SIOM)
New Zealand	SmartGates Business Travel Card (APEC) Movement Alert List (MAL)
Spain	Eurodec Schengen List Visa Information System (VIS)

Source: Legislation of the four countries study, *Migration Act 1995* (Australia), *Migration Law, General Population Law, Refugees and Complementary Protection Law* (Mexico), Immigration Act 2009 (New Zealand), *The 2/2009 Organic Law and Royal Decree 1161/2009* (Spain)

[107] New Zealand Government, *Immigration Act Review* (April 2006); Australia Government, Department of Immigration and Citizenship, *Annual Report* (2008-2009); *Ley de Migración, DOF 25/052011 [Migration Law] (Mexico)* http://www.diputados.gob.mx/LeyesBiblio/pdf/LMigra.pdf *(20/12/2012); Ley Orgánica 2/2009, de 11 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social,BOE-A-2009-19949 [Organic Law 2/2009 amending Organic Law 4/200 on the Rights and Liberties for Foreigners in Spain and their Social Integration] (Spain),* http://www.boe.es/buscar/doc.php?id=BOE-A-2009-19949 *(20/12/2012)*

[108] Australia Government, Department of Immigration and Citizenship, *Annual Report* (2010-2011); *Manual of Criteria and Migratory Proceedings of the National Institute of Migration. Acuerdo por el que se expide el Manual de Criterios y Trámites Migratorios del Instituto Nacional de Migración, DOF 29/01/2010, [Criteria and Migratory Proceedings Manual of the National Institute of Migration of the Minister of Interior of 21 September 2010] (Mexico)* http://dof.gob.mx/nota_detalle.php?codigo=5129775&fecha=29/01/2010 *(20/12/2012);* New Zealand, New IT System for Immigration New Zealand http://www.immigration.govt.nz/migrant/general/generalinformation/newitsystems/ (20/12/2012); OECD, *Recent changes in Migration Movements and Policies: country notes* (2010); see also IOM, *Migration Initiatives Appeal 2010* (2010) http://publications.iom.int/bookstore/free/Migration_Initiatives_2010.pdf (20/12/2012).

In summary, Australia has an integrated data system allowing for cross-checking among a number of databases, such as Immigration, Passports, Taxation and Social Services. There are also data exchange provisions in Australia's migration legislation, which permit information to be shared with agencies. In Mexico, the electronic system allows cross-checking of registered foreigners and refugees who hold of a valid visa and who want to change their status in Mexico. There are also provisions for APEC Business Travel Card data exchange. New Zealand's immigration legislation enables specific biometric information to be collected, stored and used to verify a foreign national's identity. There are also provisions, which permit sharing personal information, including biometric information, to national and international agencies. In addition, a foreign national's personal information can be shared with other New Zealand agencies to check his or her eligibility for publicly-funded services. Spain has EURODAC, Schengen System (SIS II) and Visa Information System (VIS)[109].

4.5.2. *Current Biometric Systems and ePassports in the Four Countries Study.* This section sets out the current operational biometric systems deployed in the context of immigration control in the four countries study. In addition, it provides the actual collection, storage and TBIF during the border control process.

These current operational biometric systems deployed in the context of immigration control in the four countries study reveal the dynamic interaction between governments, citizens and biometric industry. For instance, the continuous immigration information flow of national travellers of Australia and national travellers of New Zealand force to both countries to find a remarkable collaboration and fast track process of their national passengers in both countries creating the programme SmartGate[110]. In addition, Australian and New Zealand have introduced an online

[109] For further details, see Figure 14 above p. 122 and see Appendix H. National Immigration Policy

[110] This programme is a kiosk that checks whether Australian and New Zealand travellers are eligible for self-processing and the gate performs the identity check and clearance using Australian and New Zealand biometric passports with Basic Access Control (BAC). SmartGate is available at Sydney, Adelaide, Brisbane, Cairns, Melbourne, Perth, Gold Coast and Darwin international airports. In New Zealand, the SmartGate was implemented at Auckland International Airport for arriving passengers from Australia and New Zealand, in 2009. It is also operational for departing passengers from Australia and New Zealand at the Auckland, Wellington and Christchurch international airports. Australian Customs and Border Protection Service, SmartGate

immigration system for visas applications. This system in Australia is called Visa Entitlement Verification Online System[111] and in New Zealand this system is known as Immigration Global Management System[112].

In Spain, there are three main regional systems in operation: EURODAC, Schengen System (SIS II) and Visa Information System (VIS). The first two examples are discussed above[113] and the VIS is a centralised biometric database link to national systems that allows Schengen Member States to exchange visa data. It contains 10 fingerprints and a digital photo collected from persons applying for a visa[114].

In Mexico, there are three operational biometric databases: for refugees; foreign holders of a valid visa who want to change their status in Mexico; and, temporary and/or definitive APEC Business Travel Card (ABTC). These biometric databases are operated by the National Institute of Migration (INM). These three biometric lists are interconnected with the Consular Management Integrated System (ACIS) verifying migration real-time alerts at the time issuing visas the Electronic System for Migration Procedures (SETRAM)[115]. The overall system is known as the Integrated Migration Operations (SIOM)[116].

---

http://www.customs.gov.au/site/page5552.asp (20/12/2012); New Zealand, Customs Service website http://www.customs.govt.nz/features/bordersector/transtasmantravel/Pages/default.aspx (20/12/2012)

[111] Australia, Visa Entitlement Verification Online System http://www.immi.gov.au/Services/Pages/immiaccount.aspx (20/12/2012)

[112] New Zealand, New IT System for Immigration New Zealand http://www.immigration.govt.nz/migrant/general/generalinformation/newitsystems/ (20/12/2012)

[113] For further details, see section 4.4.6. Introduction of Biometric Systems: Regional Organisations

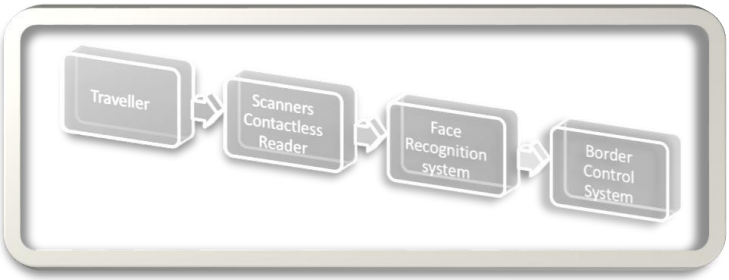
[114] Schengen Member States and Visa Information System http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm (20/12/2012)

[115] Mexican Government, National Institute of Migration, *Action Lines in Sector Programs Accountability, Transparency and Fighting Corruption committed in 2009* Final Report (2008-2012) http://www.inm.gob.mx/static/transparencia/PND/Formatos_A_y_B.pdf (20/12/2012)

[116] The INM also launched the interconnection of the Integrated Migration Operations (SIOM by its Spanish acronym) with the INM's Electronic Immigration Procedures (SETRAM by its Spanish acronym), the Consular Management Integrated System (ACIS by its Spanish acronym) of the Ministry of Foreign Affairs (SRE by its Spanish acronym). This interconnection allows Mexican consulates to automatically verify migration real-time alerts at the time of issuing visas, in order to assess the issuance of the type of visa requested. The INM also informs the SRE of the permits granted to foreigners to obtain their visas at the corresponding consulates. Instituto Nacional de Migración, "Consolida INM simplificación de trámites migratorios", (Press Release, 7 September 2011) http://www.inm.gob.mx/index.php/blog/show/Consolida-INM-simplificaci%C3%B3n-de-tr%C3%A1mites-migratorios.html (22/12/2012)

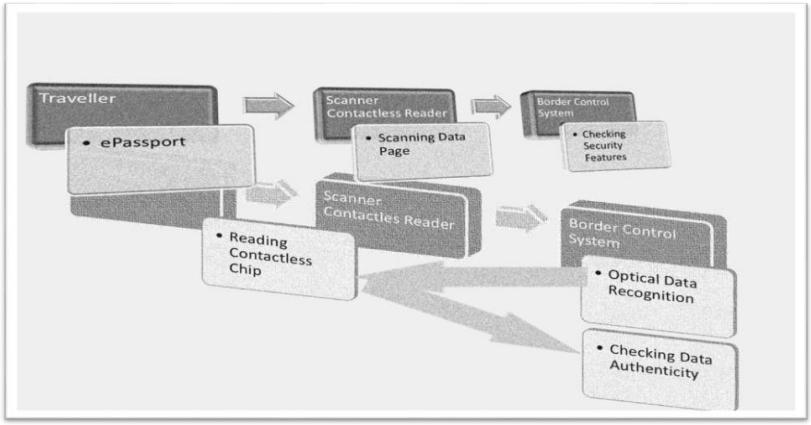
ePassports are a major component of biometric immigration systems. Generally, travellers are requested to present their ePassports and visas to the immigration officer. The following figures present the current border control process in these four countries for travellers.

Figure 15. Traveller's Complete Border Process



Where the data page of the ePassport is scanned and checked security features through the border control system. Then, the border control system using the optical recognition system[117] reads the contactless chip from the ePassport and checks data authenticity.

Figure 16. ePassport Border Control Process

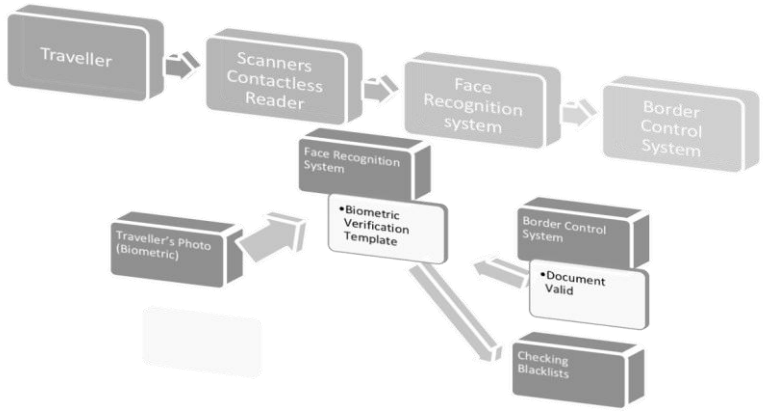


In addition, the border control officer requests to the traveller a face biometric verification where the officer takes a photograph[118] and the border control systems

[117] For further details, see Appendix C. How Biometric Systems Work
[118] Sometimes fingerprints are also requested.

validates the photograph taken in that moment with the photograph template stored in the ePassport and runs facial biometric verification through checking national blacklists and Interpol's databases[119].

Figure 17. Biometric Verification Border Control Process



The four countries study reveals that, the information collected by the border control system is stored in their national centralised immigration information databases. Technically the information collected has a specific individual purpose[120]. The use of ePassports and visas in border control process suggest that biometric travel documents are used as identity-based filters and not as a strategy to strengthen border control. The immigration information has a subsequent aggregated use within integrated data systems for cross-checking within a number of national agencies and international databases for national security and defence[121]. In Australia and New

[119] Interview with David Philp, General Manager-Passport, Department of Internal Affairs (Wellington, 25 October 2011); interview with Francisco Villanueva Díez, Deputy General Director of Information Systems and Communications for Security Matters, Spanish Minister of Interior (Madrid, 8 November 2011); interview with Alejandro del Conde, Secretary of Data Protection, Instituto Federal de Acceso a la Información y Protección de Datos [Federal Access Information and Data Protection Institute] (Mexico City, 16 November 2011); interview with Jeremy Johnson, Director National Biometric and Child Protection Services, CrimTrac Agency (Canberra, 18 October 2011); interview with Alex Webling, Policy Director, Biometrics and Identity, Attorney General's Department (Canberra, 20 October 2011) This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[120] Here the purpose is related to the Data Protection Principles theory where "the collection of information is necessary for a specific purpose". Kuschewsky, Monika (ed.), *Data Protection and Privacy Jurisdictional Comparison,* above n 16.

[121] The subsequent aggregated use is prohibit in Data Protection Principles theory where "the personal information collected shall not be used for a purpose other than that for which it was collected". Idem.

Zealand the TBIF in the context of immigration control is carried out generally by data exchange requests to specific authorities, whereas in Spain and Mexico generally have systematic data sharing. This TBIF affects privacy and data protection rights. This interference or restriction should be in accordance of the law and properly balance to decide whether privacy and data protection restrictions are necessary and justified in a democratic State.

In summary, the four countries deployed biometric systems as a measure of immigration control and there is a current TBIF between countries and international organisations. There has been a lack of public debate regarding risks of centralised biometric databases for immigration purposes, the way of exchange or share immigration information and the linkages between immigration information and international criminal databases. In addition, the absence of public scrutiny and transparency on the management of biometric databases for immigration purposes, the lack of statistics related to the exercise of access, challenges and complaints to the processing of travellers' biometric information and the way TBIF is carried out by countries and international organisations raises legal concerns not only related to possible breaches of civil liberties in general and travellers' privacy and data protection rights, in particular. But, the deployment of biometric systems and TBIF in the context of immigration control restricts individuals' privacy and data protection rights, in general. This situation needs to be assessed according to the proportionality principle to properly balance public and private interests[122].

4.5.3. *Common Control Strategies Deployed in Immigration at the International Level*. On an international level, it is possible to identify the intensification of the deployment of biometric systems and TBIF for immigration purposes. Internationally, the implementation of biometric systems in immigration policies was marked by combined international cooperation and the facilitation of cross-border information.

There are three significant areas in which the four countries study revealed biometric control strategies "as a trade-off for faster immigration processing, passengers will have to accept a system which has the potential to generate a vast amount of

[122] For further details, see Chapter 7. TransBorder Biometric Privacy Regimes: National Solutions

international traffic in their personal data"[123]. These three common areas are classified as follows:

- Amount of transborder information flow, which includes passenger pre-inspection at departing country and advance passenger information before arrival[124].

- Security civil aviation, which includes Immigration Liaison Officers (ILOS) working together with national and international law enforcement agencies to prevent irregular migration and help close down related criminal operations[125] and Airline Liaison Officers (ALOs) who are immigration inspection officers working together with airline staff in the prevention of the travel of persons with fraudulent travel documents[126].

- Carrier Sanctions within Civil Aviation Law. Nationally this legislation aims to make carriers co-responsible for embarking and delivering undocumented or improperly documented travellers with fake ePassports or without holding a

[123] Davies, S., "The Brave new world of biometric identification" (1995) 2 *Privacy Law and Policy Reporter* 30.
[124] Involves an agreement between countries, as well as between airlines and governments, permitting passenger manifests to be sent by the airlines ahead of flights to the immigration authorities of the country of destination for pre-checking before arrival. International Organization for Migration, "International Terrorism and Migration", above n 86, p. 16.
[125] Idem and *Civil Aviation Legislation (Mutual Recognition with New Zealand) Act 2006 (Cth), Ley de Aviacion Civil,* DOF 12/05/1996 [Federal Civil Aviation Law last amended on 21/05/2013] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/25.pdf (21/12/2012), *Civil Aviation Act 1990* (New Zealand) The most recent version of New Zealand Act excludes amendments that are not yet in force from 1992, 2007 and 2013 http://www.legislation.govt.nz/act/public/1990/0098/latest/versions.aspx (21/12/2012) and *Ley 21/2003, de 7 de Julio, de Seguridad Area,* BOE-A-2003-13616 [Law 21/2003 of 7 July, security aviation, last amended 1 March 2014] (Spain) http://www.boe.es/buscar/pdf/2003/BOE-A-2003-13616-consolidado.pdf (21/12/2012)
[126] Idem.

visa[127]. In Australia and New Zealand these type of sanctions are an integral part of the pre-embarkation activities abroad[128].

With their long sea borders and distance from other countries, Australia and New Zealand have been able to capitalize more on offshore clearance processes than both Mexico and Spain. Each State considers its own circumstances and adopts the policies, administrative structures and legislative measures considered to best suit their needs in protecting sovereignty and guaranteeing security.

4.6. Conclusions

The illustrative map of the biometric industry demonstrated the interaction between the government and the biometric industry and highlighted the need for the industry itself to improve their self-regulation instruments[129]. This biometric industry has a great impact on public policies dealing with immigration, but is contrasted by a lack of public debate and civil engagement regarding these policies. This chapter explored TBIF in the context of immigration mainly because it is an extensive and active area for TBIF. The chapter considered two scenarios in which TBIF may give rise to possible short and long-term challenges: one scenario is among the four countries examined and the second is between the four countries examined and their interaction with international organisations. This TBIF in immigration information flow debate should not be confined to the technical aspects of the ways in which personal data are collected, updated, retrieved, analysed and exchanged in Australia, Mexico, New Zealand and Spain. TBIF in immigration context needs to

[127] *Civil Aviation Legislation (Mutual Recognition with New Zealand) Act 2006 (Cth), Ley de Aviacion Civil,* DOF 12/05/1996 [Federal Civil Aviation Law last amended on 21/05/2013] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/25.pdf (21/12/2012), *Civil Aviation Act 1990* (New Zealand) The most recent version of New Zealand Act excludes amendments that are not yet in force from 1992, 2007 and 2013 http://www.legislation.govt.nz/act/public/1990/0098/latest/versions.aspx (21/12/2012) and *Ley 21/2003, de 7 de Julio, de Seguridad Area,* BOE-A-2003-13616 [Law 21/2003 of 7 July, security aviation, last amended 1 March 2014] (Spain) http://www.boe.es/buscar/pdf/2003/BOE-A-2003-13616-consolidado.pdf (21/12/2012)

[128] Australia and New Zealand link visa issuance abroad with entry clearance at the port of entry and departure, monitoring at the port of exit. For further details see http://www.infrastructure.gov.au/aviation/legislation/amendment/ (21/12/2012); International Organization for Migration, "International Terrorism and Migration", above n 86, p. 16.

[129] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

emphasize the lack of public engagement, transparency and scrutiny in the deployment of these biometric systems[130].

The absence of public debate; the lack of systematic studies on the biometric industry; the necessity to improve the biometric industry self-regulation; and, the current deployment of centralised biometric databases as well as the specific TBIF in immigration information control are exacerbated because the implementation of biometric systems is not adequately regulated at an international level. The roles of international (ICAO and IOM) and regional organisations (APEC and EU) are acknowledge as their established specifications and recommendations for biometric systems in travel documents and in border control systems for identification of travellers. These organisations are making efforts to create an international framework for the deployment of these biometric systems and TBIF. However, these attempts require the proactive participation for all sectors, including government, industry and social actors. An inclusive strategy is needed regarding more open public debate about technical (security) risks and limitations on civil liberties; the promotion of privacy and data protection rights; transparency and accountability on the management of these centralised national and international biometric databases.

Biometrics are not new[131], but what is new are the automated systems that allow a considerable volumes of information to be collected, stored, processed and exchanged, as discussed in preceding chapters. Even as biometric systems have been increasingly deployed, the comparative study of these four countries reveals asymmetries and convergences within TBIF in the immigration information flow context. All four countries have issued biometric passports[132], have also biometric systems for issuing visas and electronic Border Control Systems operated most of them by a border control officer. The questions arise how biometric border control processes are working, who can access immigration information, whether immigration information is reliable (integrity of data), what are the risks of data protection in third countries, are misclassifications possible of travellers from

[130] For further details, see section 1.5. The Aim and Scope of the Research
[131] For further details, see Chapter 2. Biometric Systems: What is Biometrics?
[132] For further details, see section 3.3.2. ePassport Technology: the New Generation

immigration information flow, what are the data storage restrictions in immigration control, what are the subsequent automated uses of immigration information through the interoperability of dissimilar systems at national and international levels and, finally and legally most importantly, how does TBIF in the context of immigration information flow impact individual privacy and data protection rights[133].

The current interactions of TBIF in the context of immigration information flow require a common and harmonised framework with specific rules governing the subsequent use of biometric information, cross-border rights and cross-border challenges. In addition, countries should be capable of addressing these legal challenges by balancing public interests, such as national security and defence, and individuals' privacy and data protection rights[134].

[133] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges
[134] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

CHAPTER 5.

BIOMETRICS IN CRIMINAL DATABASES: CURRENT TRANSBORDER INFORMATION FLOW

5.1. Current Biometric Criminal Databases Sketch

In addition to the study of immigration information flow, a study of the challenges of Transborder Biometric Information Flows (TBIF) arising within information flow in biometric criminal databases was also included. This part of the study has two aims, namely: to assess the accuracy of TBIF within the four countries' criminal database legal frameworks and also the adequacy of the privacy and data protection legal frameworks implemented in each country.

The comparative four countries study demonstrates that there are legal problems, limitations and challenges of TBIF in Australia, Mexico, New Zealand and Spain[1]. The analysis of TBIF involving criminal databases demonstrates that the four countries are not only collecting names, physical descriptions and different categories of offences but are also collecting biometric characteristics such as DNA, face images and fingerprints for entry on their criminal databases. Secondly, this study has revealed that reclassifications of crime on these databases have expanded to terrorism, cross-border crimes and illegal immigration. Thirdly, in order to facilitate the exchange of information, under bilateral or multilateral agreements, government agencies are allowing increasing linkage between international and national biometric criminal databases.

The four countries study confirms the existence of asymmetries and convergences in the operation and practices in relation to TBIF between criminal databases[2]. Australia, Mexico, New Zealand and Spain are collecting different types of biometric criminal information and targeting different people for inclusion. Furthermore, the types of crimes or offences are also different in each country and most legislation on

[1] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges
[2] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

the limit of time data may be kept varies in different ways from country to country. The development of biometric criminal databases policy is in transition with each country implementing it at a different pace, trying to make their priorities compatible with globalization demands.

Arguably, the operation of Interpol's databases represents best practice standards for biometric criminal databases on processing and exchanging information through their standardization of systems and methods. However, the asymmetries among national biometric criminal databases pose long and short-term challenges for a uniform TBIF at an international level. In addition, the four countries study also confirms that a poor level of scrutiny and a lack of public debate have accompanied the implementation of biometric criminal databases[3]. TBIF in the context of criminal databases needs to be developed with transparency, scrutiny and citizen engagement with input from the range of interests in civil society, including the biometric industry itself and supervisory authorities[4]. The biometric industry needs to improve its self-regulation and its engagement with ethical commitments[5]. These key points are underpinned by the theoretical requirements of Habermas and Jasanoff[6].

Furthermore, the legal challenges in the deployment of biometric systems and TBIF in criminal databases[7] requires a balance between any restrictions on individual human rights and civil liberties and any public benefits from the use of these modern scientific techniques. The proper balance between private and public interests are analysed in further chapters[8].

This chapter examines the legal and policy aspects of current biometric criminal databases. It identifies Interpol´s worldwide databases with particular reference to the four countries study. Finally, the chapter highlights the necessity to increase the

[3] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges
[4] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Einaudi, 1980); Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* (Princeton University Press, 2007).
[5] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map or Players, Products and Partnerships
[6] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4; Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* above n 4.
[7] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges
[8] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

level of transparency and accountability surrounding the expansion of biometric criminal databases.

5.2. Debates and Justifications for Transborder Biometric Information Flow and Criminal databases

Despite the deployment of biometric databases and TBIF for crime prevention, there has been little public political and legal debate or discussion[9] as compared with privacy debates related to ordinary national criminal databases. This lack of public discourse on the creation of biometric criminal databases may be interpreted as the consequence of the day-to-day conduct of society by elites[10] and fails to fulfil the theoretical requirements of Jasanoff and Habermas for public discourse on such major developments. Groups of experts can be identified, who control or advise parliaments and governments, and who hold the technical biometric "elite knowledge" without making this knowledge available to their own citizens[11].

> "State policies, correspondingly, are geared more and more toward nurturing and exploiting knowledge, with scientific knowledge and technical expertise commanding the highest premiums"[12].

In the contexts of the four countries study of Australia[13], Mexico[14], New Zealand[15] and Spain[16], there has been little public debate about criminal databases and most

[9] This is because most of the debate has been in official discourse, seminar papers, conference presentations slides and government reports.
[10] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* above n 4; Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[11] Idem.
[12] Ibidem, p. 4.
[13] Since September 11, 2001, the Australia national security agenda has emphasised counter-terrorism arrangements and developed tools needed to fight crime and provide law enforcement with DNA databases. This allows police and forensic scientists from all nine police jurisdictions to compare DNA profiles across borders and exchange information held in every state and territory. See Australia Government, CrimTrac*, Full Report (Annual Report for 2009-10)*
[14] The Mexican government's priorities are to fight crime, decrease corruption, and increase security. In 2004, 2008, 2010 and 2012, the Mexican Political Constitution was reformed to articulate the National System of Public Security (SNSP) and outline the characteristics of the competent authorities of the Federation, the Federal District –Mexico City-, 31 states and the municipalities in the National Public Security Council (CNSP).
[15] In 2003, the *Criminal Investigations (Bodily Samples) Act 1995* was amended and came into force. The Act's purpose is to expand the DNA criminal databank. The New Zealand government recognised

of the decision-making processes are dominated not only by domestic concerns, but also by international security considerations that highlight the "prevention of cross-border crimes and combat terrorism agenda"[17].

On an international level, the justification for criminal database TBIF can be summarised as follows: to solve unsolved cases by identifying persons in the DNA or Automated Fingerprint Identification System (AFIS) database of another country; to link unsolved crimes to unsolved crimes in different countries to the same –yet unidentified- persons; to establish the true identity of persons in different countries; and, to issue arrest warrants and request information regarding the whereabouts of persons[18]. In addition, following various highly publicised terrorist attacks around the world, a new argument was emerged, namely to prevent terrorism. Criminal database TBIF between countries and international agencies has become crucial not only for migration but also inter-jurisdictional police co-operation.

While biometric criminal databases may be used for TBIF to facilitate cross-border cooperation, it is important that citizens have freedom to decide their own destiny

---

that some inmates convicted prior to the commencement of the Act may be responsible for the commission of earlier unsolved crimes. Two committees of the New Zealand Parliament, the Justice and Electoral Committee and the Law and Order Committee, examined the *2003 Amendment Act* and recommended it be passed with amendments. See *Criminal Investigations (Bodily Samples) Amendment Act 2009 (09/46);* (10 February 2009) 652 NZPD 1125; *Criminal Investigations (Bodily Samples) Act 1995* No. 55 (as of 01 October 2010)

[16] There was a lack of coordination between the national and autonomous community police agencies and the proliferation of local and national criminal databases, as well as the commitments acquired by the Schengen zone and Prüm convention. Therefore, Spain was forced to reorganize its police agencies and its national information systems. See the Preamble of the *Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*, BOE-A-2007-17634 [Organic Law 10/2007 regulating the police database on identifiers obtained from DNA] (Spain) http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-17634 (21/12/2012)

[17] Multinational declarations, such as those emerging from G-7 summits, have expanded their scope and include talks concerning terrorism, the drug trade, and recently, money laundering. The G-7 Summit is an annual meeting of the heads of government of the leading seven industrial nations –the United States, Italy, France, the United Kingdom, Japan, Canada and Germany. Its agenda is predominantly economic, and is prepared by representatives of the various governments. Traditionally, a statement is released at the end of each summit that contains the agreements reached on policies. Zagaris, Bruce and Aguilar, Álvaro, "Enforcement of Intellectual Property Protection Between Mexico and the United States: A Precursor of Criminal Enforcement for Western Hemispheric Integration?" (1994) 1(5) *Fordham Intellectual Property, Media and Entertainment Law Journal* 42-123.

[18] Uthmani, Omair*, et. al.,* "Crime risk evaluation within information sharing between the police and community partners", (2011) 20(2) Information & Communication Technology Law 57-81; Tupman, W.A, "Cross-National Criminal Databases: The ongoing search for safeguards", (1995) 4(3) *Information & Communication Technology Law* 261-275.

and interests as an essential part of social and political interaction. Aragón argues that "popular sovereignty rests on the notion of political consensus", so in this case the sovereign collectively follows "the rule of the majority"[19]. However, the absence of open public debate dilutes any political consensus and the rule of the majority. In the modern concept of democracy, the principles of majority, constitutionalism and political representation are incorporated[20]. Similarly, Nino argues that government can justify a solution when all those affected by a decision have participated in discussion and have had equal opportunity to express their interests[21]. In this same sense, Águila has stated, "participation serves, at the same time, for: 1) guaranteeing collective self-governance, and 2) achieving the creation of citizens who are informed and committed to public welfare. Collective deliberation in the scope of public affairs thus generates both self-government and civility"[22]. For Habermas[23] and Jasanofff[24], public debate is essential to provide a theoretical basis for planning and to emphasize public participation, public information sharing, consensus through open and public dialogue, and avoiding or privileging experts and bureaucrats.

In Australia, New Zealand and Spain, two types of concerns were identified in national level debates. The first related to the potential of databases to affect privacy, self-determination and data protection rights; the second related to the greater benefits of linking databases and TBIF in the context of information flow in criminal

[19] Aragón, Manuel, *Constitución, Democracia y Control*, (Instituto de Investigaciones Jurídicas de la UNAM, 2002), p. 17.

[20] Thus, there is a reference to representative democracy, a regime that comes along with the formation of a liberal-constitutional State. There are several tints, according to the treatment that several authors give to democracy, we may say that the modern concept of democracy, "liberal democracy", refers to a political system based on popular power in the sense that the ownership of power belongs to *demos* while the exercise is entrusted to representatives elected on a periodic basis by the people. Therefore, the exercise of popular power resolves, to a great extent, electoral power. On the other hand, the classical theory of liberal democracy assumes that the existence of a market and individual freedoms in economic aspects is a condition for the existence of political democracy; that is, that there is a country and a market with borders.

[21] Nino, Carlos, *La constitución de la democracia deliberativa*, (Gedisa, 1997), p. 166.

[22] Águila, Rafael del *Manual de Ciencia Política* (Editorial Trotta, 5th ed, 2008).

[23] Habermas argues that the attempt to interpret popular sovereignty in procedural terms must be "carefully defined so as not to divest popular sovereignty of its radical-democratic content". He restates the principle of popular sovereignty in terms of discourse theory: "all political power derives from the communicative power of citizens". Jürgen Habermas, *The Theory of Communicative Action*, (Thomas McCarthy trans, Beacon Press, 1984).

[24] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* above n 4.

databases in order to prevent terrorism, to enhance border security and to fight organised crime[25].

By contrast, in Mexico, three opportunities for national public debate were identifiable but were not realised. Debates were possible but did not eventuate. In Mexico, there was no public discussion or debate about linking databases nationally or internationally[26]. The three possible opportunities of public discussion were:

1) First, in 2007, the Mexican government proposed the design of procedures, manuals and standards, as well as of the architecture for the development of biometric data[27]. No public debate accompanied this proposal.

2) Secondly, the Ministry for Public Security (SSP)[28] developed a National Program of Public Security (PNSP) for 2008-2012, with seven strategic objectives, one of which was called "Platform Mexico"[29]. This Ministry was dissolved in December 2012 when a new Government administration assumed power. All the powers and projects of the former SSP were reassigned to the Ministry of Internal Affairs.

[25] Interview with Charlotte Epstein, Professor, University of Sydney (Sydney, 26 October 2011); Interview with Katina Michael, Associate Professor, University of Wollongong (Sydney, 21 February 2012); Interview with Pilar Nicolas, Professor, University of Deusto (Bilbao, 10 November 2011) This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[26] Interview with Ernesto Villanueva Villanueva and Issa Luna Pla, Professors, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [Legal Research Centre of the National Autonomous University of Mexico] (Mexico City, 23 November 2011) This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[27] It is possible to conclude this from the Mexican State of the Nation address. Mexico Government, Presidential Office, *First Report regarding the Application of the National Development Plan 2007-2012*, Rule of Law and Security (2007) http://pnd.presidencia.gob.mx/pdf/PrimerInformeEjecucion/1_3.pdf (21/12/2012)

[28] The Secretariat for Public Security (SSP) was the Federal Civil Service body which aimed to preserve freedom, order and public peace, and to safeguard the integrity and rights of the people by preventing the commission of crimes. This Secretary or Minister no longer exists as of 1 December 2012.

[29] Conectividad a la Plataforma México [Connectivity Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-cpm-10_1.pdf (21/12/2012)

3) Thirdly, in February 2008, the Mexican government applied to the Inter-American Development Bank for technical cooperation to develop the strategic plan for "Platform Mexico Project" (ME-T1094)[30]. Again, no debate ensued.

However, it is possible to find media releases promoting the "Platform Mexico Project"[31] and the advantages of this linkage between Mexico and Interpol[32]. From papers presented at seminars and conference presentation slides presented by the Mexican authorities, it is possible to identify an official policy position. Nevertheless, there have been no critics of the Platform Mexico nor any public debates or academic discussions about TBIF between Mexican biometric criminal databases and international criminal databases.

In essence, the four countries examined share a comprehensive lack of public debate and a poor level of scrutiny on TBIF in the context of information flow in criminal databases. These countries share the same objective to "improve international cooperation". The failure to foster a robust public discussion about the implementation of biometric criminal databases, and the relative exclusion of key actors from different areas from participating in the development of regulatory frameworks is a major deficiency. By comparison and in stark contrast, privacy and data protection regime debates have been very different and openly discussed with public participation, reaching consensus for guidelines and ethical commitments nationally and internationally.

[30] The technical cooperation requested for "Platform Mexico" also included a budget for internal organisation of the Ministry of Public Security. Mexico Government, Minister of Public Security, *Platform Mexico,* 1st Report of Duty 2006-2007 (2007) http://pdba.georgetown.edu/Security/citizensecurity/Mexico/evaluaciones/InformeLabores-plataformamexico.pdf (21/12/2012) Today this Ministry no longer exists (as of 1 December 2012); all functions and duties related to "Platform Mexico" have been reassigned to the Ministry of Internal Affairs.

[31] Otero, Silvia, "Conectarán Plataforma México con Interpol", *El Universal*, Mexico City, 10 de junio de 2008 http://www.eluniversal.com.mx/notas/513761.html (21/12/2012)

[32] Interpol, "Mexico to link its databases with INTERPOL's in unique new partnership" (Media Release, 3 June 2008) http://www.interpol.int/News-and-media/News-media-releases/2008/N20080603 (21/12/2012)

5.3. Policy Development: The Transition to biometric criminal databases

There has been a steady transition from the use of traditional criminal databases towards the implementation of biometric criminal databases. Biometric criminal databases were the essential foundation for international linkages and TBIF. During this transition stage, it is possible to track three key elements in the actual policy development: the biometric information collected; the reclassification of crimes; and, the actual exchanges and linkages between databases.

5.3.1. *Information Collected*. The first element in this transition is the information collected in criminal databases: from nominal or textual characteristics to biometric characteristics. The purposes for which biometric information is collected is also relevant to this discussion.

Nowadays, criminal databases not only collect names, dates of birth, sex, physical descriptions and categories of offences, but also include some biometric characteristics like DNA, face images, fingerprints, iris patterns or voice.

Each country's national criminal legislation sets the criteria for collecting, accessing, storing and deleting information and database management. As criteria are set at the national level, it is possible to find asymmetries among criminal databases reflected at the international level. Information collection criteria are not determined by scientific or technological standards, but by these national legal prescriptions. At this point, countries are collecting biometric information: a) related only to crimes; b) related to crimes and other biometric data; or c) related to crimes, biometric data and more information as a result of the linkage among biometric criminal databases. A distinct and common characteristic related to the varied information collected, during this transition phase is that different countries are collecting biometric data but then start to use it for other purposes[33].

[33] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

Accordingly, the development of national criminal database frameworks, as well as and international linkages, should be negotiated with the highest degree of transparency and the involvement of data protection authorities[34].

5.3.2. *Reclassification of Crimes*. The second element in this transition stage is the reclassification of crimes. Because of the need to combat terrorism, cross-border crimes and illegal immigration, countries require international co-operation. This requires a consistent classification of crimes at a national level.

In Europe, for example, the Schengen Information System II[35] is a biometric list of wanted and unwanted persons designed to prevent cross-border crimes and illegal immigration. The Prüm Convention[36] authorised the expansion of the classifications of information collected to create a more extensive database of biometric characteristics compiled to tackle not only cross-border crimes, but also terrorism and illegal immigration.

- *Terrorism*

After terrorist attacks in 2001, countries developed a "unique global instrument to enhance national, regional and international efforts to counter terrorism"[37]. International cooperation is continuing and expanding at an international level[38].

At a national level, countries introduced amendments to their criminal laws and prosecution systems to include terrorism as a transnational crime and terrorism-related offences. For example in New Zealand, terrorism-related offences include terrorist bombing, financing of terrorism, recruiting members of terrorist groups, participating in terrorist groups, hijacking, other crimes relating to aircraft, crime

[34] For further details, see Chapter 8. Conclusions
[35] For further details, see Appendix F. Schengen Information System
[36] For further details, see Appendix G. Prüm Convention
[37] *United Nations Global Counter-Terrorism Strategy*, GA Res 60/288, UN GAOR, 116th sess, 117th plen mtg, Agenda Item 46, UN Doc A/Res60/288 (20 September 2006, adopted 8 September 2006).
[38] There are 13 international conventions http://www.un.org/terrorism/instruments.shtml (21/12/2012) These instruments were developed under the auspices of the United Nations, its specialized agencies and the International Atomic Energy Agency (IAEA) and are open to the participation of all Member States.

relating to international airports, and wrecking[39]. In Mexico, the definition of terrorism, as a crime, embodies an historical aspect related to treason. The Mexican Federal Criminal Code classifies the crimes of national terrorism and international terrorism[40].

Terrorism and counter-terrorism have been widely debated, but a legal classification problem arises when discussion turns to 'terrorist activity'. This type of activity is included in criminal databases because it encompasses 'crime prevention' justifications[41]. But the term is not specific and precise and the current definition of 'terrorist activity'[42] depends on individual assessment. Habermas might explain this as "the intent to legitimate political decisions in a less rational way"[43]. Such assessments affect civil liberties.

- *Cross-border crimes*

Cross-border crimes are classified as 'transnational organised crimes'[44] and are treated as domestic criminal offences. These offences may directly or indirectly threaten individuals but also social, cultural, economic and political regimes. Activities considered cross border crimes are: drug trafficking, people trafficking, trafficking in firearms, smuggling of migrants; money laundering[45] and terrorism,

[39] *Criminal Investigations (Bodily Samples) Amendment Act 2003* (New Zealand)
[40] Therefore, since 1917, all crimes related to treason to homeland like terrorism, sabotage, conspiracy, rebellion, mutiny, sedition or insurrection are considered as serious offence by the *Código Penal Federal*, DOF 14/08/1931 [Federal Criminal Code, last amendment 14/06/2012] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf (21/12/2012)
[41] *Criminal Code Act 1995* (Cth); the Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE-A-1995-25444 [Organic Law 10/1995 Criminal Code] (Spain) https://www.boe.es/buscar/doc.php?id=BOE-A-1995-25444 (21/12/2012); *Criminal Investigations (Bodily Samples) Amendment Act 2003* (New Zealand) and *Código Penal Federal*, DOF 14/08/1931 [Federal Criminal Code, last amendment 14/06/2012] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf (21/12/2012)
[42] Reviewing the Australian, Mexican, New Zealand and Spanish criminal legislation, it is possible to define terrorist activity as situations in which "groups or individuals operate entirely inside a country, attempting to influence the government or population to effect political or social change".
[43] Habermas, Jürgen (1980), "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[44] There is no single accepted definition of transnational organised crime. Mueller, Gerhard O. W. "Transnational Crime: Definitions and Concepts," (1998) 4 *Transnational Organized Crime* 13-21; Williams, Paul D. *Security Studies. An Introduction,* (Routledge, 2008); Collins, Alan, *Contemporary Security Studies,* (Oxford University Press, 2007); Barkawi, Tarak and Laffey, Mark (eds.) "The post-colonial moment in security studies" (2001) 32(2) *Review of International Studies* 329-352.
[45] *United Nations Convention against Transnational Organized Crime,* opened for signature on 15 November 2000 (entered into force on 29 September 2003).

among others transnational crimes[46]. These are the typical offences that trigger inclusion in international criminal databases.

However, as noted, there is no consistent international classification. Each country decides which criminal offences should be included in their criminal databases and what information will be exchangeable. Policy making is undertaken at a national, rather than an international level.

- *Illegal immigrants*

Migration, including illegal immigration, is a complex issue[47] that has an impact on the economy and social life of any countries. Most countries are designing their migration policies based on economic and social benefit[48] with little open and public dialogue consensus through real deliberative democracy[49]. Migration discourse centres on two areas: the first relates to combating people smuggling[50], and the second to border security in terms of avoiding the threat of terrorists entering a country. Many countries place illegal immigration in the same policy debates about terrorism and cross-border crimes, in this transition stage of policy making. In this context, if countries continue to strengthen their migration policies, there is a possibility that some countries could categorize illegal immigration as criminal activity.

[46] Intellectual property crime, cybercrime, maritime piracy, stolen motor vehicles, environmental crime, counterfeit medical products, firearms trafficking, stolen works of art and stolen travel documents.
[47] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[48] Like Weber's "bureaucratic domination" concept in which bureaucracy is impersonal and "depends upon regular income, and hence at least a portion on a money economy and money taxes". Gerth, H. H. And Wright Mills, L. (ed.) *From Max Webber, Essays in Sociology*, (Rutledge, 2009).
[49] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4; Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States*, above n 4.
[50] For Interpol "people smuggling simply implies the procurement, for financial or material gain, of the illegal entry into a state of which the individual is neither a citizen nor a permanent resident. Trafficking is distinct from smuggling insofar as the traffic of human beings involves the exploitation of the migrant, often for purposes of forced labour and prostitution" http://www.interpol.int/Crime-areas/Trafficking-in-human-beings/Trafficking-in-human-beings (21/12/2012).

5.3.3. *Exchanging and Linking Databases to enable Transborder Biometric Information Flow (TBIF)*. The third element of this transition is the way in which TBIF is carried out, the exchange of information by specific request and the actual linkage of databases by systematic sharing data between countries for international cooperation.

In both cases of TBIF, the exchanging or linking of national criminal information with any international agency or country means not only sharing information, but also its processing personal information. In the last two decades, TBIF has been possible, mainly in Europe[51] through Interpol[52] with background checks, for example based on textual information searches by name, aliases, date of birth and sex. Nowadays, TBIF is a reality everywhere, and searches can be performed, not only on textual information but on DNA, fingerprints, iris, face images and other biometric characteristics.

Concerning international cooperation and assistance, there are challenges in consistency of criteria and creating open and representative procedures in specific institutional contexts. There are different forms of international cooperation and assistance: bilateral or multilateral treaties, and/or cooperation with international or regional organizations or agencies that facilitate the TBIF by exchanging specific information or linking different databases. In the global era, the TBIF should to be possible via the Internet, across the world using biometric systems without any problems posed by the range of the Roman alphabet, the Cyrillic alphabet or Chinese characters. Biometric characteristics should be insensitive to text characters or language translation.

[51] At that time, systems included the Schengen Information System, SIRENE, EUROPOL, EURODAC, Customs Information System (CIS) and the Visa Information System (VIS).
[52] Since 1987, Interpol has operated its own Criminal Intelligence Database or Criminal Information System (ICIS).

5.4. Criminal Databases: A Comparison of Standards and Consistency

Criminal databases have been studied for a long period and some of the policy issues considered include: a) people registered by type of crimes or offences, b) limitations on the period of time the data may be kept, c) authorised user access profiles, d) how often information can be accessed and for what purposes, e) interoperability between databases, and f) data protection at a different pace than that of how the information actually flows[53].

Nowadays, many international agencies and organisations with different aims but related roles, such as Europol and Interpol operate criminal databases. There are also different systems, with similar objectives but different structures, which manage criminal information for crime prevention and migration purposes, such as EURODAC[54], and the Schengen Information System II[55], expanded by the Prüm Convention[56]. There has not been widespread debate on how do these organisations and systems work; how recommendations are made and implemented; or, how specifications for biometric criminal databases are established[57]. In this section, the implementation of biometric criminal databases is examined through the lens of Interpol's databases and a comparison of national cases, in the four countries study, to identify the differences between countries and Interpol in terms of what and how information is collected.

[53] Romeo Casabona, Carlos Maria (ed), *Bases de datos de perfiles de ADN y criminalidad*, (Cátedra Interuniversitaria, Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, 2002).

[54] For further details, see Appendix E. Eurodac Introductory Information

[55] For further information, see Appendix F. Schengen Information System

[56] For further information, see Appendix G. Prüm Convention. Member States have direct access to the databases of another Member States. Authorities responsible for immigration and administration of aliens have direct access. In addition, Prüm DNA database and AFIS database are compatible with INTERPOL databases. *Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,* [2008] OJ L 210/1.
Also, it will be possible to link with the Platform Mexico because of the interoperability of Mexican databases and INTERPOL databases.

[57] Most of the literature explains the EU treaties that creates these databases in general, but regarding the management, operation and statistics of these international biometric systems are minimal.

5.4.1. *Interpol Databases with Worldwide Coverage*. Interpol performs an important function as the only police organisation with worldwide coverage[58]. The Interpol intelligence System (ICIS) differs from other systems, as it is international in nature while others are European systems[59]. Interpol does not have teams of detectives with supranational powers to travel around investigating cases in different countries. Interpol officers are bound by the laws of each nation and Interpol itself respects national sovereignty that permeates the execution of its tasks and operations[60]. However, the TBIF is governed by Interpol's own structures and procedures.

Each Member State of Interpol provides and maintains a national Interpol office as a National Central Bureau (NCB). Interpol has developed the I-24/7 Global Police Communication System to connect National Central Bureaus to the Interpol General Secretariat[61]. This in turn creates a global network for exchanging police information and providing member country law enforcement authorities with instant and direct access to a wide range of criminal information through a variety of databases and other services[62].

All databases, except one with child sexual abuse exploitation images, are accessible through the I-24/7. The main databases available are: nominal data, notices, stolen and lost travel documents, stolen administrative documents, stolen

[58] Interpol has 190 member countries. For its purpose, policy aims, legal bases and organisational overview, see the official web site at http://www.interpol.int/ (21/12/2012). Another important reason for choosing Interpol and not Europol can be found in the observation made by the European Union Committee of the House of Lords: "Europol has only recently established its own information system, after extensive delays. Neither agency has sufficient relevant expertise in managing large-scale information systems. In the case of Europol there might be a conflict of interest, or at least a perception of one, between its role as a user of the service and as a service provider, particularly since it is supposed to have access only to limited categories of data". European Union Committee, House of Lords, *Schengen Information System II (SIS II),* 9th Report of Session 2006-07 (2007).

[59] Since 1987, Interpol has operated its own Criminal Intelligence Database or Criminal Information System (ICIS). The aim was to improve methods of storing and retrieving information on crimes and criminals, to speed up replies to Interpol National Central Bureau (NCB) inquiries, and give the Interpol Police Division immediate, direct access to the computerised files.

[60] For example, the Mexican Constitution has embodied a concern for Mexican sovereignty throughout its history.

[61] Located in Lyon, France.

[62] Interpol's overview website http://www.interpol.int/INTERPOL-expertise/Overview (21/12/2012)

motor vehicles, stolen works of art, DNA profiles, fingerprints, fusion task force[63], fast disaster victim identification[64] and counterfeit payment cards[65].

Countries can exchange not only nominal data, but also DNA, fingerprints and palmprints. Interpol rules on processing and exchanging information[66] were revised in 2009 and Interpol launched the "I-link", the first operative system developed to improve the exchange of information between member countries[67]. "I-link" is a technological tool that ensures data consistency. It includes an option for storing queries in the database and receiving an alert if a match is found on the data at a later date.

The international DNA database and the Automated Fingerprints Identification Systems (AFIS) used by Interpol are centralised databases[68]. For example, these Interpol biometric criminal databases are compatible with the Combined DNA Index System software (CODIS)[69] used by the Federal Bureau of Investigation (FBI), Schengen Information System II and the Platform Mexico[70].

[63] Interpol Fusion Task Force website http://www.interpol.int/Public/FusionTaskForce/default.asp (21/12/2012)
[64] Interpol Fast and Efficient International Disaster Victim Identification website http://www.interpol.int/INTERPOL-expertise/Databases/FASTID/FAST-and-efficient-international-disaster-victim-IDentification (21/12/2012)
[65] Interpol counterfeit Payment Cards website http://www.interpol.int/Crime-areas/Financial-crime/Payment-cards (21/12/2012)
[66] For example, the requirements for fingerprints, palmprints and also DNA.
[67] Interpol Data Exchange website http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-link (21/12/2012)
[68] The requirements for fingerprints and palmprints are: to adopt and adhere to the standard ANSI/NIST (Type 4 images if it is for ten print processing, and type 7 or 15 if it is palmprint processing), use the Acquisition Guidelines for National AFIS, use the international fingerprint or palmprint matching tool (INT-1), use the fingerprint image capture system, and use the fingerprint image compression (WSQ Gray Scale).
[69] The CODIS version 5.7.3., called "Interpol Export Tool", will facilitate member countries' extraction of DNA profiles ready for data input through the Interpol DNA Gateway.
[70] In 2008, Mexico linked their national criminal databases with Interpol by connecting Platform Mexico to Global Police Communications System I-24/7. This means that when a Mexican police officer updates a national criminal database, it will automatically update Interpol data. At the same time, it will also record, store, organise, consult and use Interpol databases on wanted persons, stolen and lost travel documents and stolen motor vehicles as it updates its own databases. Interpol, "Mexico to link its databases with INTERPOL's in unique new partnership", above n 32 and Otero, Silvia, "Conectarán Plataforma México con Interpol", *El Universal*, above n 31.

Regarding Stolen and Lost Travel Documents (SLTD), the Interpol database holds information about travel documents and identity cards reported lost or stolen in 161 countries[71]. A significant characteristic of the SLTD databases is that most of the travel documents are biometric travel documents. For example: APEC Business Travel Cards, Schengen Zone Visas, Interpol personnel ePassports and the four countries study. This database allows immigration and border control officers to validate a suspect travel document in a matter of seconds[72].

In 2010, Interpol launched a new database called Fast and Efficient International Disaster Victim Identification (FastID), which is a centralised database to identify and link missing people and unidentified bodies by means of decentralised access available through "I-link" [73].

5.4.2. *Interpol Database Best Practices*. Interpol rules on processing and exchanging information allow countries to exchange not only nominal data, but also DNA, fingerprints and palmprints[74]. Interpol's biometric criminal databases are capable of use as identification systems when used to search for and compare sample profiles. For security reasons, Interpol operates a system of standardized methods, loci and systems[75]. Interpol has developed rules on conditions and basic procedures according to which information must be processed in accordance with Article 2 of Interpol's *Constitution and the Universal Declaration of Human Rights*.

[71] Interpol Stolen and Lost Travel Documents (SLTD), http://www.interpol.int/INTERPOL-expertise/Databases (21/12/2012)
[72] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[73] Interpol Data Exchange website http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-link (21/12/2012).
[74] For example, the requirements for fingerprints and palmprints, as well as for DNA.
[75] Interpol actively participates with international standards committees focusing on forensic DNA and other biometric characteristics, for example the European Network of Forensic Science Institute (ENFSI) http://www.enfsi.eu/index.php (21/12/2012) and International Organization for Standardization (ISO) http://www.iso.org/iso/home.html (21/12/2012)

- *Standardisation of methods.*

Interpol has been a leader in standardization of data. There are four main documents that standardise the information that Interpol collects, stores, retrieves and exchanges. These documents are the "[r]ules on the processing of information for the purposes of international police co-operation"[76], "[i]mplementing rules on the processing of information for the purposes of international police co-operation"[77], the "[r]ules governing access by an intergovernmental organization to the Interpol telecommunications network and databases"[78] and the "[r]ules on the Control of Information and access to INTERPOL's files"[79].

Standardisation includes the purposes for which information is processed[80], the role of the General Secretariat[81], the role of entities in the processing of information[82], the organization's databases[83], the right to process information, confidentiality of information, processing security, general conditions for processing information[84], general procedure for processing information, cases in which the General Secretariat must consult the source of an item of information, deadline and postponement of the deadline for examining the need to hold on to certain information, the provision on modifying, blocking or destroying a piece of information[85] and their consequences[86]. It includes also the conditions and instances in which an item of information may be

[76] *Rules on the Processing of Information for the purposes of international police cooperation (RPI)* (2008).
[77] *Implementing rules on the processing of information for the purposes of international police co-operation* (2009).
[78] *Rules governing access by an intergovernmental organization to the Interpol telecommunications network and databases* http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts *(*21/12/2012)
[79] *Rules on the Control of Information and access to INTERPOL's files* (2010).
[80] This includes processing for international police co-operation purposes, as well as for any other legitimate purpose.
[81] This includes the request for information and conclusion of co-operation agreements.
[82] This includes the role of National Central Bureaus in their relations with the authorized national institutions, provisions of information, control of information by the information source and the use of information.
[83] This includes different categories of databases in addition to conditions for setting up and deleting databases.
[84] This includes provisions relating to particularly sensitive information, to extracted information, to processing information for other legitimate purposes and to the processing of notices.
[85] This includes the initiative of an entity other than the source of an item of information and provisions specifically concerning notices.
[86] This includes action taken by the General Secretariat and the retention of elements of an item of information.

provided, methods of providing information, the retention of requests for information received and of the communications themselves.

Interpol has also developed rules for direct access, downloading and interconnection; provisions for an authorised entity to directly record information on an autonomous database; requisitioning and providing information in urgent situations; provisions related to monitoring the processing of information in Interpol files; and, access to such information.

- *Standardisation of loci.*

Interpol has also developed a set of standardized loci which are used by 185 member countries to exchange biometric information. This Interpol set is called the Interpol Standard Set of Loci (ISSOL). While the ISSOL is identical to the European Standard Set (ESS)[87], the ISSOL is recommended for easier international comparison as the minimum requirement for entry is 6 of the 24 STR (Short Tandem Repeat) plus the gender marker Amelogenin[88].

- *Standardisation of system.*

In the case of DNA databases, Interpol encourages countries to use the "I-link" as their main operative system to run the I-24/7 portal on which all databases are accessible online[89]. The "I-link" is accessible to all member countries upon acceptance of: the Communication Security Charter[90], the use of the international DNA matching tool[91] and compliance with the international data exchange format

[87] The requirements for DNA databases are to: use the international DNA standard (ISSOL - This is the standard set of loci that Interpol recommends for easier international comparison. Locus [pl. loci] is the physical location of a gene [or DNA region of interest] on a chromosome), to accept Interpol DNA charter, use the international DNA matching tool (©IPSG Lyon), use the international data exchange format (IPSG .xsd / .xml) and use the Secure Telecommunication Network (I-24/7).

[88] Interpol (2009), *Interpol Handbook on DNA Data Exchange and Practice,* Appendix 1: Interpol Standard Set Of Loci: ISSOL, p. 84 http://www.interpol.int/INTERPOL-expertise/Forensics/DNA (21/12/2012)

[89] Except the database on child sexual abuse exploitation images.

[90] *Rules on the Control of Information and access to INTERPOL's files* (2010) http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts (21/12/2012)

[91] Interpol (2009), *Interpol Handbook on DNA Data Exchange and Practice* http://www.interpol.int/INTERPOL-expertise/Forensics/DNA (21/12/2012)

programme[92]. In the case of fingerprints and palmprints databases, all member countries must adopt and adhere to the ANSI/NIST standard and use the Acquisition Guidelines for National AFIS. Countries also must use the international fingerprint or palmprint matching tool, the fingerprint image capture system and fingerprint image compression.

In the view of this study, Interpol, through these three standardization processes of methods, loci and systems, represents the current international best practices for criminal databases in the ways Interpol collects, stores, retrieves and exchanges criminal information in TBIF.

5.4.3. *National Criminal Databases: A Case Study*. The Interpol system stands in contrast to national criminal databases. Each country's particular criteria for the collection, access, storage, deletion of information and database management is set by its national criminal law.

The asymmetries among criminal databases are reflected on an international level. This section will give a brief description of criminal databases in Australia[93], Mexico[94], New Zealand[95] and Spain[96]. The aim is to identify how countries use their

[92] *Rules on the Processing of Information for the purposes of international police cooperation (RPI)* (2008) http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts (21/12/2012)

[93] The Australian government, in co-operation with state and territory governments, has established a DNA criminal investigation system. These criminal databases are hosted by CrimTrac, which was established on 1 July 2000 to develop the technology required to give police ready access to information needed to solve crimes. http://www.crimtrac.gov.au/about_us/index.html (21/12/2012) Australia has eight national criminal systems, but only two share DNA and Biometric information with the Department of Immigration and Citizenship (DIAC).
The eight national criminal systems are: the National Criminal Investigation DNA Database, the National Automated Fingerprint Identification System, the Australian National Child Offender Register, the National Police Reference System, National Vehicles of Interest, the National Firearm Licence and Registration System, the National Police Checking Service, and the National Name Index.

[94] In 2009, Mexico modernised its National Communication Network and restructured its National Information System, linking fifteen national databases and centralising information from states and municipalities onto eight new systems, which includes four biometric criminal databases. This project is known as "Platform Mexico". The databases are : the Unified Criminal Information System (SUIC), the Unified Penal Institution Administration System (SUAP), Global Policing Operations System (SIOP), Geographic Information System (SIG), Automated System for Organized Crime Analysis (SAADOM), Comprehensive Organized Crime Information System (SIICDO), Uniform Statistical System for Analyses on Drug Manufacturing and Trafficking (SEUNAD), National Call Centre for Crime Reports (CND).
Mexico Government, Inter-American Development Bank, *Strategic Planning Project "Platform Mexico,* Technical cooperation profile (2008)

biometric criminal databases and to emphasize the need to move to greater standardization.

For the purposes of this four countries study national comparison, four issues are taken into account: targeted people and types of crimes, duration of time for data storage, user access profiles and exchanges of data through TBIF.

- *Targeted people: type of crimes or offences*

The inclusion of specific categories of targeted people is based on particular types of crime. Government agencies may believe that the "greater the amount of individuals included in the database, the better results will be obtained in the resolution of criminal cases"[97]. Most legislation bases inclusion on the number of years in prison (5 years) rather than on the crime itself, for example, robbery, homicide or sexual abuse[98]. In Spain, for example, is a combination of both the crimes itself and "serious" crimes[99].

---

http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=1397559 (21/12/2012) or http://www.iadb.org/en/projects/project,1303.html?id=ME-T1094 (21/12/2012) The technical cooperation of "Platform Mexico" had a total cost (historical) of USD $275,280.

[95] *Criminal Investigations (Bodily Samples) Amendment Act 2003* (New Zealand) governs police and Environmental Science Research (ESR) working methods for DNA sampling and testing, including the taking of reference samples for specific investigations and the taking of samples from individuals for inclusion in the National DNA Databank. The National DNA databank has two databases and by comparing the two databases, possible suspects can be identified and crimes can be linked. http://www.esr.cri.nz/competencies/forensicscience/dna/Pages/DNAdatabank.aspx (21/12/2012)

[96] In 2007, *the Organic Law 10/2007*, which governs the comprehensive police database on identifiers obtained from DNA, came into force. This new database Comprehensive DNA Criminal Database is based on the Combined DNA Index System developed by the Federal Bureau of Investigation (FBI), which includes samples of DNA or other body tissues taken from convicted offenders, arrestees, legal detainees, forensic or unidentified human remains and missing persons. Articles 3 and 4 of the Organic Law 10/2007 regulating the comprehensive database police on identifiers obtained from the DNA. *Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*, BOE-A-2007-17634 [Organic Law 10/2007 regulating the police database on identifiers obtained from DNA] (Spain) http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-17634 (21/12/2012) Before 2007, there was no specific legal provision in Spain for regulating evidentiary DNA in the criminal law system.

[97] Romeo Casabona, Carlos Maria (ed.), *Bases de datos de perfiles de ADN y criminalidad*, above n 53.

[98] Idem and *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) of the European Parliament and of the Council*, [2002] OJ L 201/37, *Communication from the Commission to the Council and the European Parliament - Towards enhancing access to information by law enforcement agencies (EU information policy),* [2004] COD 2004/0429.

[99] Article 3.1.a of the Organic Law 10/2007, "serious" crimes and "in case those affecting life, liberty, indemnity or sexual freedom, integrity of the people, and property, provided those crimes were

Australia allows DNA registration from suspects, serious offenders, convicted persons and volunteers[100]; New Zealand allows DNA registration from any suspect and for any recordable offence –total of 78 offences[101], serious offenders, convicts and volunteers; and Spain allows DNA registration from convicts, serious offenders and volunteers. The following figure shows the people included in national biometric criminal databases currently in use.

Figure 18. People Targeted for Criminal Databases

Who can be included?					
Country	Suspects	Serious offenders	Convicted	Volunteers	Others
Australia	Yes	Yes	Yes	Yes	No
Mexico	Yes	Yes	Yes	Yes	Yes
New Zealand	Yes	Yes	Yes	Yes	No
Spain	Yes	Yes	Yes	No	No

Source: Legislation of the four countries study. *Crimes Act 1994* (Australia); *General Act on the National Public Security System* (Mexico); *Criminal Investigations (Bodily Samples) Amendment Act 2003* (New Zealand); *Law 10/2007 regulating the comprehensive database police on identifiers obtained from the DNA* (Spain)

The Mexican regime allows the registration not only of suspects, serious offenders, convicted persons and volunteers, but it also includes random voice samples obtained, even without the consent of the people recorded over the phone who utter key words that trigger the voice biometric identification system developed by the company Speech Technology Center[102].

committed using force on things, or violence or intimidation in persons, as well as in cases of organized crime". *Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*, BOE-A-2007-17634 [Organic Law 10/2007 regulating the police database on identifiers obtained from DNA] (Spain) http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-17634 (21/12/2012

[100] *Crimes Act 1914 (Cth)*

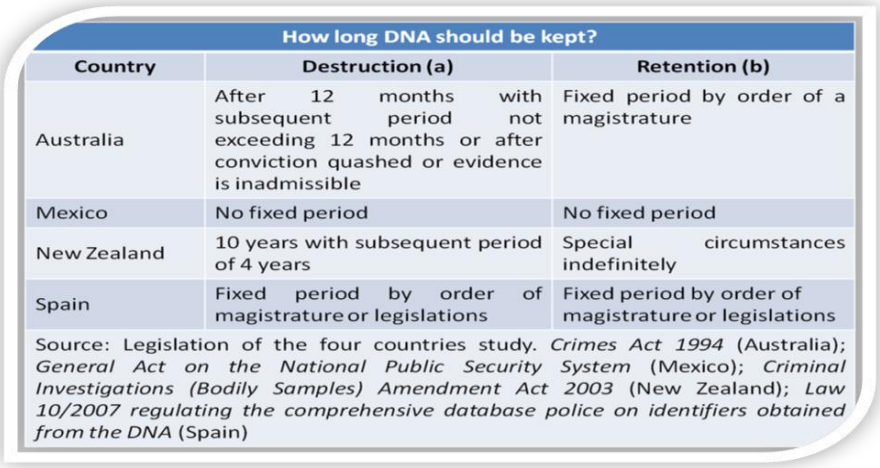
[101] Examples of these 78 crimes in New Zealand include: smuggling migrants, terrorist bombing, financing of terrorism, recruiting members of terrorist groups, participating in terrorist groups, hijacking, other crimes relating to aircraft, crime relating to international airports, wrecking, attempting to wreck. *Criminal Investigations (Bodily Samples) Amendment Act 2003 (New Zealand).*

[102] This company was identified in Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and http://www.software-russia.com/ (20/12/2012)

- *Duration of Time for Data Storage* [103]

A country's retention of biometric information is frequently controversial, and there may be more concerns surrounding linkages with international biometric databases. National legislation set different limits on the time during which data may be retained. In Australia, the information collected for the National Criminal Investigation DNA Database (NCIDD) may be held for as long as deemed necessary[104]. In New Zealand, DNA profile will be held on the database on any person convicted of a serious offence[105]. In Mexico, the *General Act on the National Public Security System* establishes the regime for criminal databases and does not include any provision on the destruction or retention of samples, nor for deletion of information held in criminal databases[106]. Finally, Spain specifies times for retention of data, dependent on the seriousness of the crime[107]. The following figure illustrates the duration of DNA data retention:

Figure 19. Duration of DNA Stored



How long DNA should be kept?

Country	Destruction (a)	Retention (b)
Australia	After 12 months with subsequent period not exceeding 12 months or after conviction quashed or evidence is inadmissible	Fixed period by order of a magistrature
Mexico	No fixed period	No fixed period
New Zealand	10 years with subsequent period of 4 years	Special circumstances indefinitely
Spain	Fixed period by order of magistrature or legislations	Fixed period by order of magistrature or legislations

Source: Legislation of the four countries study. *Crimes Act 1994* (Australia); *General Act on the National Public Security System* (Mexico); *Criminal Investigations (Bodily Samples) Amendment Act 2003* (New Zealand); *Law 10/2007 regulating the comprehensive database police on identifiers obtained from the DNA* (Spain)

[103] Romeo Casabona, Carlos Maria (ed), *Bases de datos de perfiles de ADN y criminalidad*, above n 53.
[104] *Crimes Act 1914 (Cth)*, s 23YDAE.
[105] *Criminal Investigations (Bodily Samples) Act 1995* No 55 (as at 01 October 2010), Public Act, s 2(1), s 7(b)(xiii).
[106] *Ley General del Sistema Nacional de Seguridad Pública*, DOF 02/01/2009 [General Act on the National Public Security System, last amended on 28/12/2012] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf (21/12/2012)
[107] Article 9 of *Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*, BOE-A-2007-17634 [Organic Law 10/2007 regulating the police database on identifiers obtained from DNA] (Spain) http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-17634 (21/12/2012)

- *User access profiles*

It is essential to have legislative provisions regulating authorised access to criminal databases. Legislation should specify which national authorities have access, their corresponding clearance levels to search data, the recording of these searches and purpose of these searches. In most cases, regulation should include practices and procedures for training staff. This type of regulation is in operation in Australia, New Zealand and Spain.

In Australia's National Criminal Investigation DNA Database (NCIDD), only the state or territory that supplied the DNA profile can identify the person to whom the profile belongs. However, for the National Automated Fingerprint Identification System (NAFIS), the police as well as the Department of Immigration and Citizenship (DIAC) have access to manage and identify unlawful non-citizens and to aid in the processing of onshore protection visa applications.

In New Zealand, the 2003 *Criminal Investigations (Bodily Samples) Amendment Act* allows access to the National DNA Database, the Crime Sample Database and the Automated Fingerprint Identification System (AFIS) by authorities responsible for immigration and administration of foreign nationals[108].

In Spain, the *Unified DNA Criminal Database*[109] allows nationwide access by national and local (autonomous communities) police agencies and the National Centre of Intelligence. At an international level, judicial, prosecutor or police authorities will be authorised to make access applications[110].

[108] Storage of more than 430,000 original sets of fingerprints.
[109] This database includes DNA or other body tissue samples taken from convicted offenders, arrestees, detainees, forensic scenes, unidentified human remains and missing persons. Articles 3 and 4 of the *Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN*, BOE-A-2007-17634 [Organic Law 10/2007 regulating the police database on identifiers obtained from DNA] (Spain) http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-17634 (21/12/2012)
[110] Ibidem, article 7 a), b) and c) of the *Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN* This provision was included in anticipation of the issue being addressed in international treaties.

In Mexico, the Platform Mexico contains criminal information databases[111], the national voice biometric database[112] and the Police and Security Staff Member Database[113]. All the technical protocols related to these databases are publicly available at the *Manual for Information Collection and Exchange[114]; the Connectivity Platform Mexico*[115]; the *Integration, Consultation and Updating of Fingerprint Records[116], Logical Security Platform Mexico[117]* and *People Identification System Using Voice Analysis*[118]. It is important to note that the *Manual for Information Collection and Exchange* applies to the federal public administration, including law enforcement areas.

[111] The Criminal Biometric Fingerprints database and DNA Database contain information of individuals who were suspects, were arrested, are in prison, were released or had escaped as set forth in two laws: *Ley General del Sistema Nacional de Seguridad Pública*, DOF 02/01/2009 [General Law of National System of Public Security, last amendment 28/12/2012] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf (21/12/2012) and *Ley de la Policía Federal*, DOF 25/05/2011 [Federal Police Law] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LPF.pdf (21/12/2012)

[112] Speech Technology Center, "World's first nationwide Voice Identification System deployed in Mexico by Speech Technology Center (Russia)" (Media Release, 4 June 2010) http://speechpro.com/media/news/2010-06-03 (21/12/2012) this company was identified in Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

[113] This contains information on members of public security institutions at all levels and jurisdictions. The information includes the identity and adscription of public officials, such as biometric fingerprints, biometric photographs, biometric handwriting, DNA, educational background, employment history and professional qualifications. Mexico Government, Minister of Public Security, *Platform Mexico,* 1st Report of Duty 2006-2007 (2007) http://pdba.georgetown.edu/Security/citizensecurity/Mexico/evaluaciones/InformeLabores-plataformamexico.pdf (21/12/2012)

[114] *Acuerdo por el que se dan a conocer el Manual de Captura de Información y el Manual de Intercambio de Información*, DOF 21/09/2006 [Manual for Information Collection and Exchange] http://www.normateca.gob.mx/Archivos/32_D_1092_07-11-2006.pdf (21/12/2012)

[115] Conectividad a la Plataforma México [Connectivity Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-cpm-10_1.pdf (21/12/2012)

[116] Integración, Consulta y Actualización del Registro de Huellas Dactilares [Integration, Consultation and Updating of Fingerprint Records] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-rehd-10_1.pdf (21/12/2012)

[117] *Seguridad Lógica de la Plataforma México* [Logical Security Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-slpm-10_1.pdf (21/12/2012)

[118] *Sistema de Identificación de Personas Mediante Análisis de Voz* [People Identification System Using Voice Analysis] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-sav-10_1.pdf (21/12/2012)

- *Transborder of information (interoperability / linkage)*

In Australia, New Zealand and Spain, there are privacy principles related to cross border data flows; avoiding the disclosure of personal information when collecting information from third countries. However, there are no published reports available on the privacy norms governing criminal databases. In Mexico, the *Manual of Procedure for Collection and Exchange of Information for Mexican Public Administration Agencies*, which governs criminal databases[119], is publicly available.

In the four countries study, neither protocols nor reports on TBIF involving criminal databases were available at the time of writing. This thesis argues that biometric criminal databases regulatory frameworks should involve robust public policy debates.

5.5. Conclusion

Crime prevention is one of the critical areas where it is legally permissible for governments to limit privacy and data protection rights, but the question is how far it is permissible to do so and with what justification[120]. This chapter explored the current operation of biometric criminal databases, which collect not only names, physical descriptions and categories of offence, but also some biometric characteristics such as DNA, face images and fingerprints. This chapter presented an overview of two scenarios in which TBIF may arise in the short and long-term: 1) between each of the four countries, and 2) between the countries examined and their interaction with international organisations. This chapter analysed Interpol databases with world coverage and best practices through Interpol's standardisation in methods and systems. Interpol databases are the most significant because of the 190 countries that interact with them. The comparative four countries study revealed asymmetries and convergences in TBIF between criminal databases and the lack of public scrutiny or debate about these developments.

[119] *Acuerdo por el que se dan a conocer el Manual de Captura de Información y el Manual de Intercambio de Información*, above n 112.
[120] For further details, see Chapter 7. Transborder Biometric on Privacy and Data Protection: National Solutions

This chapter demonstrated the distinct civil liberty concerns in relation to the growth of these databases. Despite these concerns, for and against linkage between criminal databases, most tend to favour linkage[121]. Nevertheless, TBIF in the context of crime prevention needs to be assessed in terms of the lack of public debate and secrecy surrounding the deployment of biometrics and TBIF. The current information flow in biometric criminal databases confirms two modes of transborder information in the four countries study: the exchange of specific information and linkage of biometric databases. In addition, the lack of public available statistics related to the exercise of access, rectification, cancellation and opposition to the processing of TBIF in the context of crime prevention, the absence of transparency and accountability in the management of biometric criminal databases strongly supports the need for proper supervisory and accountability measure in the deployment of biometric systems and TBIF in the context of crime prevention to secure individuals´ privacy and data protection rights[122].

[121] An important characteristic regarding the kind of sources consulted on linkage databases and the exchange of information is that most of the discussion has taken place in seminar papers, conference presentations slides, government reports, a few submissions or opinions and journal articles.
[122] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges

CHAPTER 6.

TRANSBORDER BIOMETRIC INFORMATION FLOWS: LEGAL CHALLENGES

6.1. Outline of Legal Challenges of Transborder Biometric Information Flows

This thesis has examined and identified the legal challenges, limitations and concerns of Transborder Biometric Information Flows (TBIF) in the contexts, of immigration and criminal databases. The comparative four countries study has demonstrated that the deployment of biometric systems in immigration control and in crime prevention is essentially concerned with greater efficiency in border processing, stopping illegal immigrants, fighting cross border crimes and preventing terrorism[1].

This chapter discusses the challenges identified in both immigration information flow[2] and information flow in criminal databases[3] contexts. Through the comparative four countries study, critical short and long-term controversies are presented in this chapter as common legal challenges for TBIF in individual countries and the world at large.

A uniform and harmonised TBIF was expected to be found in both immigration information flow and information flow in criminal databases; however, the TBIF in the four countries examined is not consistent with respect to the information collected, stored, processed and exchanged. In addition, the comparative study also showed a lack of common practices for TBIF in immigration information flow and information flow in criminal databases. These legal challenges are: who can access, data reliability (integrity), data protection in third party countries, the classification of individuals, data storage restrictions, subsequent use of the information through

[1] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges
[2] For further details, see Chapter 4. Biometric Systems in the Context of the Transborder Immigration Flow
[3] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

interoperability and its impact on privacy. Six of these legal challenges have been studied since the 1980s and have yet to be resolved.

The subsequent automated use of information through interoperability is a recent legal challenge instigated by the biometric industry in November 2011[4]. Nevertheless, this thesis argues that the subsequent chain of linkages to other databases involving different agencies from different fields, nationally and internationally, challenges and undermines individuals' privacy and data protection rights[5]. International privacy and data protection regime considers that personal information should only be collected for a specific purpose and be used solely for that specific purpose[6].

From the beginning, this thesis has argued the development of biometric systems and TBIF has lacked public scrutiny from three perspectives: first, the lack of public debate regarding the introduction of biometric systems in public sector; second, the necessity to improve the self-regulatory instruments of biometric industry; and, finally, the need to implement transparency and accountability jointly with the deployment of biometric databases. These will help not only to reduce legal challenges, but also to improve the level of privacy and data protection frameworks.

This chapter sets the legal challenges of TBIF in the two contexts of immigration and criminal databases. The chapter analyses and assesses these immigration and criminal databases scenarios for TBIF and identifies common national and international legal challenges in these contexts. This chapter argues that the absence of a robust framework of transparency and accountability is a major common legal challenge for TBIF. This chapter calls for a balance between private and public interest in TBIF[7].

[4] This is the date when the ANSI/NIST-ITL standard was release by the National Institute of Standards and Technology.
[5] For further details, see section 1.4 Hypothesis
[6] Kuschewsky, Monika (ed.), *Data Protection and Privacy Jurisdictional Comparison,* (Thomson Reuters, 2012).
[7] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions.

6.2. Transparency and Accountability as Control Mechanism

This section focuses more closely on the lack of transparency and accountability surrounding the deployment of biometric systems in immigration and criminal databases. This thesis proposes the use of transparency and accountability as a mechanism to control the deployment of any biometric system, especially for use in immigration control and crime prevention[8]. As Jasanoff has argued "It is no longer possible to deal with such staple concepts of democratic theory as citizenship or deliberation or accountability without delving into their interaction with the dynamics of knowledge creation and use"[9].

This thesis discussed, the way in which the legal, ethical and political discourse justifying the use of biometric systems for immigration control and crime prevention has been handled in the four countries studied are not consistent with the minimum standards expected in constitutional democratic States[10]. Furthermore, according to the theoretical requirements (public debate, transparency, scrutiny) set by Jasanoff[11] and Habermas[12], the governments of these four countries have failed not only to openly discuss this topic, but also have failed to involve different actors and agencies in the discussion and deployment of biometric systems and TBIF.

Citizens' participation has been insignificant because they cannot easily access publicly available biometric technology information deployed against them. In addition, the relative exclusion of various actors from collaborating in the development of regulatory frameworks, such as supervisory authorities, the biometric industry itself, non-governmental organizations (NGOs), academic privacy groups and data protection activists.

---

[8] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges

[9] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* (Princeton University Press, 2007), p. 6.

[10] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow and Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

[11] Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* above n 9.

[12] Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Euinaudi, 1980).

For a long time, secrecy has been the approach of most countries' governmental activities. However, transparency and accountability have recently expanded around the world with the introduction of Freedom of Access Information Acts (FOIA). In addition, transparency and accountability improves trust and credibility between citizens and governments. In Mexico, for instance, the *Federal Transparency and Access to Governmental Public Information*[13] (known as Mexican FOIA) is used by civil society organisations to fight corruption[14]. Transparency and accountability policies, supported by FOIA, are essential to address and reduce national and global challenges in the deployment of biometric system and TBIF policies[15]. It is essential for citizens to have the information needed to guarantee effective control in the exercise of their rights. In this way, citizens can exercise their power of control, an essential element in any democratic constitutional State.

Control must be understood as the exercise of public offices: "the term 'control' focuses on the revision, supervision, surveillance, prevention and correction measures that countries have provided through its several regulations"[16]. Through transparency[17] and accountability[18], citizens should learn about the issues on which they are to decide, as well as become, to a certain extent, more knowledgeable about the issues assigned to their competence[19].

---

[13] *Ley Federal de Transparencia y Acceso a la Información Pública,* DOF 11/06/2002 [Federal Transparency and Access to Governmental Public Information last amended on 08/06/12] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf (21/12/2012)

[14] Ackerman, John and Sandoval Ballesteros, Irma, "The global explosion of freedom of information laws" (2006) 58 *Administrative Law Review* 85-130.

[15] For further details, see section 6.3. Mapping Common Challenges of Transborder Information Flow

[16] Nieto, Santiago, *et. al.*, *Control externo y responsabilidad de los servidores públicos del Distrito Federal,* (UNAM, 2005), p. 23.

[17] Villanueva, Ernesto, *Derecho de la información*, Porrua-Camara de Diputados-Universidad de Guadalajara, 2006), pp. 69-72.

[18] Accountability has a historical explanation that can be found in Article 15 of the Declaration of the Rights of the Man and of the Citizen of 1789, in which the social right to accountability and the obligation of public officers to be accountable are provided: "The community has the right to demand an account of his administration to every public agent". *Déclaration des droits de l'homme et du citoyen* [Declaration of the Rights of the Man and of the Citizen] (France) According to Luis Carlos Ugalde, accountability is nowadays defined as the permanent obligation from authorities or agents to inform the people under their authority, the acts they carry out as a result of the authority delegation performed through a formal or informal agreement, and which implies penalties due to failure to comply with it. Ugalde, Luis Carlos, *La rendición de cuentas en los gobiernos estatales y municipales*, (Auditoría Superior de la Federación, 2002).

[19] Sartori, Giovanni, *Homo Videns, la sociedad teledirigida,* (Taurus, 2004), p. 163; Aragón, Manuel, *Constitución, Democracia y Control*, (Instituto de Investigaciones Jurídicas de la UNAM, 2002); Nino, Carlos, *La constitución de la democracia deliberativa*, (Gedisa, 1997), p. 166; Habermas, Jürgen *The*

In the context of immigration information flow, it should be possible to access information related to the public entities and organisations themselves, their management and budgets. In the four countries study, only Mexico updates its immigration statistics on a monthly basis and provides statistics on the number of requests regarding the exercise of the right to access, to rectify (correct), to delete (cancel or block) or object (oppose) the processing of personal data[20]. By comparison, Spain updates its immigration information every three months, while Australia and New Zealand only update after every census. These three countries do not have publicly available statistics on the exercise of rights to access personal data[21].

In the context of criminal databases, the four countries studied allow access to information related to the public entities and organisations themselves and their management. Mexico, however is the only country that posts its budget on a website while the other three countries make their budgets available in their annual reports. These reports tend to focus more on organisational activities, database performance and statistical trends in the number of searches deployed by agencies rather than on the number of requests to access the stored information and the number of requests to exercise the right to rectify, cancel or oppose personal data in criminal databases. Importantly, of the four countries, Mexico and Spain require that any databases created or handled by any governmental agencies or bodies, including national security databases, must be registered with and/or by their respective privacy agencies[22].

Theory of Communicative Action (Thomas MCCarthy trans, Beacon Press, 1984); Habermas, Jürgen *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (William Rehg trans, MIT Press, 1996).

[20] Individuals' exercising their ARCO rights, which give individuals to control effectively their personal information. Kuschewsky, Monika (ed.), *Data Protection and Privacy Jurisdictional Comparison,* above n 6.

[21] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[22] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

A constant feature in the four countries study was the lack of public debate about the biometric systems deployed in the context of immigration control and crime prevention.

Internationally, the lists of national authorities authorised to search for data reflect the divergences and differences identified in the four countries study[23]. There are few statistics on the operation of European databases and the numbers and types of alerts are poorly organized and not very revealing[24].

In summary, in order to promote trust and reduce concerns between citizens regarding these technologies, biometric systems should be implemented in conjunction with transparency and accountability policies and with the introduction of Freedom of Access Information Acts (FOIA). It is important to publicly discuss the deployment of these technologies, including their benefits and risks.

6.3. Mapping Common Challenges of Transborder Biometric Information Flow

This section examines national and international legal concerns within the context of TBIF in immigration information flow and information flow in criminal.

It was possible to identify four common biometric databases deployed in both contexts for immigration control and crime prevention. These biometric databases are used by border control agencies in the four countries examined. Border controls are placed at seaports, airports and land crossing ports. Mexican and Spanish immigration departments access facial image and fingerprint databases whereas Australian and New Zealand immigration departments access iris pattern and facial image databases. The figure below shows the biometric databases exchange between agencies at a national level[25].

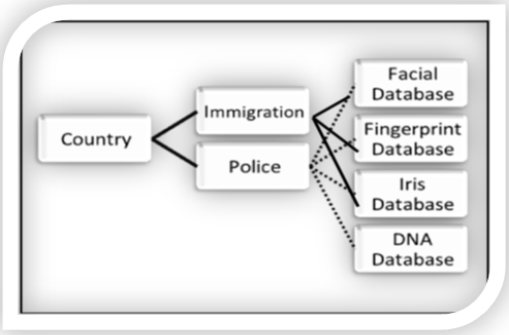
---

[23] Kabera, Stephen, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation,* (Nartinus Nijhoff Publishers, 2008), p. 222.

[24] Council of European Union, "SIS and SIRENE statistics-Guidelines to Collect Data" (2010) http://www.statewatch.org/news/2011/jan/eu-council-guidelines-data-sis-sirene-17436-10.pdf (22/12/2012)

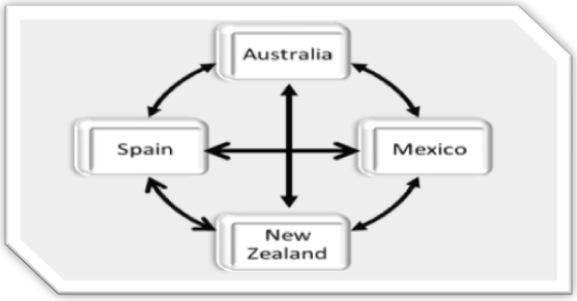
[25] This chart is based on the current operational biometric systems identified in the four countries study.

Figure 20. Biometric Databases



TBIF comprises two types of scenarios with the same domestic legal concerns but on a global scope. The first scenario is the linkage or exchange of biometric information between the requesting country and another country. The figure below shows the first scenario where cross border biometric databases between four countries examined.

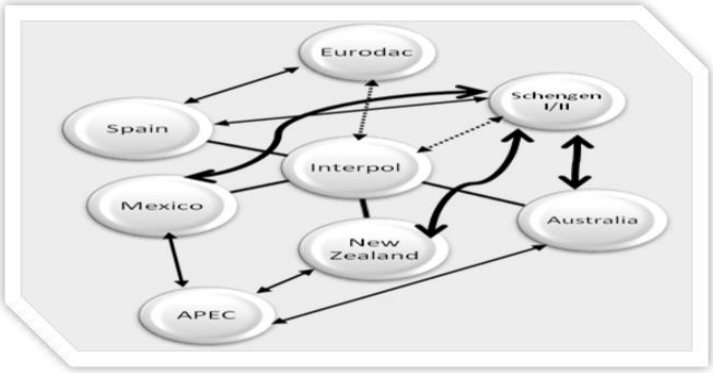
Figure 21. TBIF between Four Countries Study[26]



The second scenario is the deployment of regional and international biometric databases linked to national biometric databases. The figure below shows the second scenario in which cross-border international biometric databases exchange information among the four countries examined, Interpol, Eurodac, the Schengen Information System and APEC.

[26] Figure elaborated from diagrammatic illustration from Shoniregun, Chalres A., and Crosier, Stephen, *Securing Biometrics Applications* (Springer, 2008) p. 132

Figure 22. TBIF between Countries and International Databases[27]



On a national level, the deployment of biometric databases raises legal challenges about who can access the information, the reliability of the data (integrity), data protection for third parties, the classification of individuals, data storage restrictions, its subsequent use and its impact on privacy. On an international level, legal challenges are magnified because the impact on privacy and data protection affects a wider range of people compared to those listed in national databases. The levels of TBIF for purposes of immigration control and crime prevention in a globalised world is increasing.

6.3.1. *Who Can Access the Information*? A major challenge relates to who can access the data at national and international levels. Within a country, it is important to provide an effective legal and ethical regulatory framework. A national regulatory framework should clearly and coherently specify who can access database information, the type of information different people can access, how often information can be accessed and for what purposes the information can be accessed[28]. Worldwide related agreements on processing and exchanging personal information are often brief and generalized, but should cover the same issues. In fact, there are recommendations about establishing a registry of those who access this data and a record of the purposes for which the information was accessed,

[27] Figure elaborated from diagrammatic illustration from Shoniregun, Chalres A., and Crosier, Stephen, *Securing Biometrics Applications* (Springer, 2008) p. 133.
[28] Romeo Casabona, Carlos Maria (ed), *Bases de datos de perfiles de ADN y criminalidad*, (Cátedra Interuniversitaria, Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, 2002).

including a public list of national and international authorities who are allowed to access it and the circumstances under which they do/did so[29].

In the four countries examined, the legal framework specified which border control agencies have access to biometric databases[30]. It is important to note that in the case of Mexico, the provisions are established at a regulatory level. However, its legal framework does not mention the staff position (person) who has access, to what information and how often that information can be accessed.

The regulatory framework should be comprised of protocols or manuals for all border control agencies with access clearance. However at the time of writing this thesis, only one of the four countries examined has these types of procedural rules for immigration control and crime prevention public available for public viewing.

Mexico's manuals of procedures, standards and protocols developed for the criminal databases[31] are available to the public, as are its manuals of procedure for the collection and exchange of information for Mexican public administration agencies[32]. These include the following criminal protocols: *Connectivity Platform Mexico*[33]; *Integration, Consultation and Record Updating Fingerprint*[34]*; Logical Security Platform Mexico*[35] and *People Identification System Using Voice Analysis*[36]*.*

[29] *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) of the European Parliament and of the Council*, [2002] OJ L 201/37 and *Communication from the Commission to the Council and the European Parliament - Towards enhancing access to information by law enforcement agencies (EU information policy),* [2004] COD 2004/0429.

[30] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[31] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

[32] *Acuerdo por el que se dan a conocer el Manual de Captura de Información y el Manual de Intercambio de Información, DOF 21/09/2006 [Manual of Collection and Exchange of Information]* http://www.normateca.gob.mx/Archivos/32_D_1092_07-11-2006.pdf (21/12/2012)

[33] Conectividad a la Plataforma México [Connectivity Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-cpm-10_1.pdf (21/12/2012)

[34] Integración, Consulta y Actualización del Registro de Huellas Dactilares [Integration, Consultation and Record Updating Fingerprint] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-rehd-10_1.pdf (21/12/2012)

[35] *Seguridad Lógica de la Plataforma México* [Logical Security Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-slpm-10_1.pdf (21/12/2012)

[36] *Sistema de Identificación de Personas Mediante Análisis de Voz* [People Identification System Using Voice Analysis] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-sav-10_1.pdf (21/12/2012)

Meanwhile, in Australia, New Zealand and Spain, the only documents of this type that are made public are the annual reports posted on their respective official websites[37]. But some of these reports simply contain information about the organisation itself, its management, database performance and statistical trends related to the number of searches deployed by agencies while other reports include the operational budget. Hence, it is impossible to know who has access to the biometric databases and how such access is regulated.

These protocols should be publicly available not only because it will increase trust between citizens and governments, but citizens will also be informed and it will shape public opinion on biometric systems[38].

In addition, knowing who has access, how often biometric databases are accessed and for what purposes they can be accessed improves the protection of privacy and data at both national and international levels. It also works as a control mechanism in instances of interagency co-operation. As mentioned, border control entails work between various agencies, including immigration, police, taxation and social services departments. Domestically and globally, the ideal scenario would be to have a proper balance between border control agencies.

6.3.2. *Data Reliability and Integrity***.** The second major challenge centres on the exchange of information and its reliability at national and international levels. On a national level, it is vital for the collection, storage and classification of personal data to be accurate, complete and up-to-date. These elements are essential if governments want to generate confidence and trust between the competent authorities and citizens. However, these aspects are even more important on an international level because there are higher expectations of facilitating cross-border co-operation between countries and international agencies[39].

[37] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

[38] As argued by Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 12 and Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9.

[39] For Europol, for example, the Member State or third parties supplying such data shall notify Europol of the purpose for which they are supplying the information and of any restriction on use of that

In immigration, for example, the implementation of passenger identification systems requires fast and seamless TBIF to ensure that details of arriving passengers are received in advance (in the case of arriving flights)[40] and linked with the corresponding biometric travel documents to allow border control agencies to determine their response.

Mexico uses the *Manual for Information Collection and Exchange* and Spain uses the European Commission common standards for information exchange in immigration[41] whereas the procedures for Australia and New Zealand were not publicly available at the time of writing.

The regulatory framework consists of protocols or manuals for any border control agency that collects, stores, retrieves, classifies and updates biometric databases for the national and international exchange of biometric information. In both contexts, the integrity and consistency of biometric databases are basic requirements.

6.3.3. *Data Protection in Third Party Countries*. The third major challenge involves procedures for data protection in third party countries at any level. In relation to data protection, third party means any person, public authority, agency or body other than the data subject, controller, processor or other person authorised to process

---

information, its deletion or destruction, including possible access restrictions in general or specific terms. However, the Europol Convention established the provision that transfers should only be made to third parties –countries and bodies- that provide an adequate level of data protection. Interestingly, Australia interacts with Europol. *Agreement on Operational and Strategic Cooperation between Australia and the European Police Office*, signed 20 February 2007, ATS (entered into force according article 22).

[40] This information is provided by airlines, websites or tourism agencies when travellers book their ticket. There are some joint recommendations from the World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO) about advance passenger information (API). See Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[41] *Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals*, [2003] OJ L 157/15; *Regulation (EC) 1683/95 laying down a uniform format for visa,* [2003] OJ L164/14; *Regulation (EC) 333/2002 on a uniform format for forms for affixing the visa issued by Member States to persons holding travel documents which are not recognised by the Member State drawing up the form*, [2002] OJ L 53/23; *Regulation (EC) No 444/2009 of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States,* [2009] OJ L 142/6; *Resolution (74)29 related to the protection of individuals vis-à-vis electronic data banks,* adopted 20 September 1974.

biometric information. The sequence of this biometric information process carried out by third parties poses risks related to the misuse or disclosure of information.

It is important to note that biometric information flows are possible through two methods of exchanging information or linking databases nationally and internationally. Australia and New Zealand exchange information between them by specific requests whereas Mexico and Spain have linked their databases exchanging systematic information. In the four countries examined, the privacy and data protection legal framework considers limitations for collecting data from third parties. An assessment of the privacy and data protection legal frameworks of these countries will be given in later chapter[42].

Therefore, this challenge should be taken into account both countrywide and worldwide since data protection practices must be consistent to achieve an adequate level of privacy and personal data protection, and even more so when third parties are involved.

6.3.4. *Classification of Individuals.* The fourth major challenge relates to the classification of individuals at national and international levels. It is important to note that travellers and criminals have been previously classified in order to be listed and enrolled in national databases. This challenge extends worldwide. Thus, the classification of travellers will be discussed, followed by the classification of criminals.

Travellers are generally classified according country categories or type of visas[43]. However, the classification of travellers is implemented when travellers arrived at the border control and show their travel documents for identification. Border control

[42] For further details, see Chapter 7. Transborder Biometric on Privacy and Data Protection: National Solutions

[43] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

systems at seaports, airports or land crossing ports are organised by classification for identification of travellers[44].

The classifications of travellers in the four countries examined are completely different. The following figure shows how the countries examined organise the identification of travellers based on the type of travel documents. This classification should not be confused with the different types of visas (tourist, business, student and so on).

Figure 23. Summary of the Classification of Travellers

Classification of travellers (summary)				
Holders with biometric travel document	**Countries require visa to enter**			
	Australia	**Mexico**	**New Zealand**	**Spain**
European Union	Yes	No	No	No
US and Canada	Yes	No	No	No
Holders with electronic travel document	**Australia**	**Mexico**	**New Zealand**	**Spain**
Latin-American	Yes	Some	Some	Some

It is important to note that Australia is the only country that operates a universal visa scheme[45]; in other words, for Australia it does not matter whether travellers hold a biometric or an electronic travel document.

The classification of travellers raises two types of debate. The first highlights the argument of possible discrimination by identifying travellers according to their classification[46]. However, countries have already established immigration legal frameworks and rules concerning the issuance of different types of visas in accordance with their national security policies. In addition, countries have the right

[44] Kabera, Stephen, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation,* above n 23, p. 363.
[45] Australia deploys different systems at several points to ensure the traveller is properly authorised to enter: Universal Visa System (UVS), the Airline Liaison Officer (ALO) network, Advanced Passenger Processing (APP) and border processing at entry points at Australian airports and seaports. It is important to note that Australia's PP Advanced Passenger Processing System Check-in Guide is publicly available. Department of Immigration and Citizenship, *Australia's PP Advanced Passenger Processing System Check-in Guide,* (October 2008).
[46] Chelowinsky, Ryszard, *Borders and discrimination in the European Union*, ILPA- Immigration Law Practicioners' Association (2002). http://www.ilpa.org.uk/data/resources/13281/ilpa_mpg_borders.pdf (22/12/2012)

to exclude a person's entry to the country in the case of possible threats to personal safety and/or national security[47].

The second claim is that biometric passports and visas are used as identity-based filters and not as a strategy to strengthen border control. Considering that countries have implemented common control strategies for passenger identification systems, this presents an undue impact on privacy if biometric characteristics are requested from travellers in order for them to enter. This argument will be analysed under the Civil Law principle of proportionality and its equivalent Common Law reasonableness standard in the following chapter[48].

In the case of criminals, governments generally seek the inclusion of criminals based on the number of years in prison rather than on the crime itself. However, the challenge revolves around three national concerns: the volume of people included or listed; the interpretation of the offence and the use of different profiling systems. In the four countries examined, more asymmetries were found than similarities.

It is important for common practices in the classification of individuals to be apply both nationally and internationally.

6.3.5. *Data Storage Restrictions*. The fifth major challenge concerns the restrictions on how long data may be stored at national and international levels. Three of the four countries examined have clear provisions on their restrictions on the storage, deletion and destruction of personal information kept in national centralised databases. It is important to recall that Mexican criminal legal framework does not contain provisions regarding data storage restrictions. In the four countries examined, more asymmetries than similarities were found[49].

[47] Heath Wellman, Christopher and Cole, Phillip, *Debating the Ethics of Immigration, Is there a Right to Exclude?* (Oxford University Press, 2011).
[48] For further details, see Chapter 8. Conclusion
[49] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

Each country is responsible for ensuring that the data collected for or exchanged from its national databases to other countries or international agencies is not retained longer than necessary, either in the country or abroad. The ideal would be to have standardized practices on biometric data storage restrictions or deletion.

6.3.6. *Subsequent Automated Use of Information*. The sixth major challenge consists of the subsequent automated use of information through the interoperability of dissimilar systems at national and international levels. This challenge is not about technology itself. However, interoperability is only possible by using a common standard. A standard is a common format that provides quality, security and durability in the exchange of information between similar systems. In other words, a standard makes it possible to exchange information between different systems[50].

Before 2011, there were six common standards developed by the biometric industry for compatible systems and used for specific purposes. Most of these common standards were also required by international agencies. These six common standards were: ICAO, INTERPOL, FIPS201, ISO, ANSI, NIST, ITL and NCITS. At that time, interoperability between databases was only possible by using one of these standards with compatible systems.

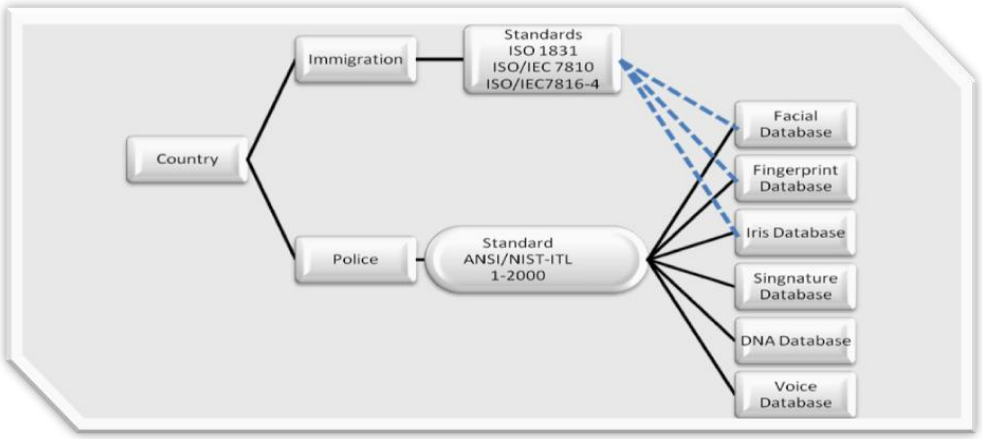
Linkages between compatible systems are allowed because they are used for similar activities. The European Union called it the “principle of availability” and “equivalent access”, invoking key elements for exchanging information[51]. However, there are restrictions to link civilian databases with law enforcement databases nationally and internationally. One example of this is the Europol Convention, which establishes that the Europol processing system must under no circumstances be linked to any

[50] Wing, Bradford, “Future of ID, Developments in Standards & Critical Projects”, in Wise Media, (Paper presented at the Tenth ID World International Congress, Milan, 3 November 2011).
[51] *Communication from the Commission to the Council and the European Parliament – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice,* [2005] OJ C 236/24. See also, *Communication from the Commission to the Council and the European Parliament - Towards enhancing access to information by law enforcement agencies (EU information policy),* [2004] COD 2004/0429.

other automated processing system, except for the automated processing systems of the national units[52].

The standards were classified according to civilian activities and law enforcement or military activities. Therefore, travel documents and national identity cards use ICAO and ISO standards[53], whereas the police use ANSU, NIST, ITL and NCIST[54]. The figure below shows the different standards used for immigration and criminal databases.

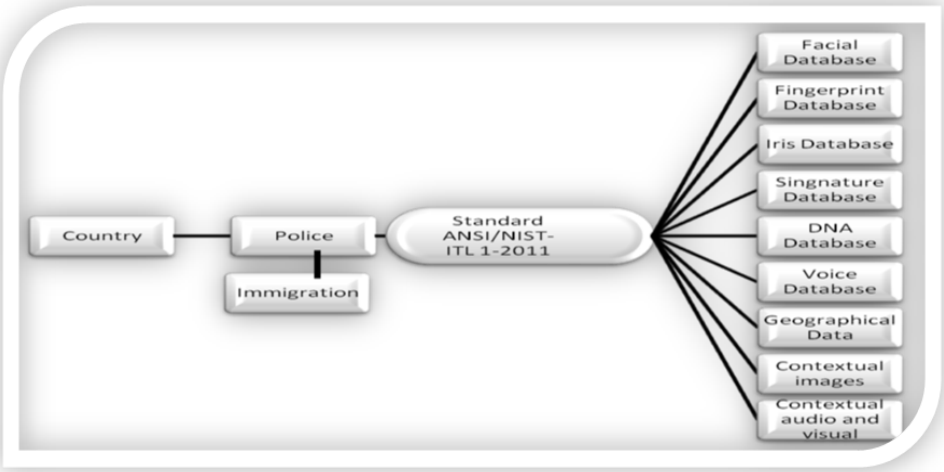
Figure 24. Biometric Standards for Databases[55]



In November 2011, a new standard was released: the ANSI/NIST-ITL 1-2011. This standard allows not only the interoperability between dissimilar systems like immigration databases and criminal databases, but also the storage, transmission and process of geographical data (position locations), associated contextual images and audio and visual data[56]. The figure below shows the subsequent automated use of biometric information.

[52] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31.
[53] The format allows specific biometric modality for facial, iris, fingerprints and signature biometric characteristics.
[54] The format allows specific biometric modalities for identifying marks, tattoos, DNA, fingerprints, iris, face, signature and voice biometric characteristics.
[55] Figure elaborated from diagrammatic illustration from Shoniregun, Chalres A., and Crosier, Stephen, *Securing Biometrics Applications* (Springer, 2008) p. 84.
[56] National Institute of Standards and Technology http://www.nist.gov/itl/iad/ig/ansi_standard.cfm (22/12/2012)

Figure 25. Subsequent Automated use of information[57]



This standard may pose a future challenge because it facilitates the subsequent automated use of biometric information and other types of personal data between different agencies from different fields nationally and internationally, as this thesis argues[58]. In addition, this challenge may have an impact on other challenges such as access of data, data reliability and data protection in third party countries, noting that the information collected from third parties too must also be accurate and up-to-date. It is possible that the information collected for subsequent use may not be complete or up-to-date.

Furthermore, as this thesis argues, one major principle for the international privacy regime should be that personal information should be collected for a specific purpose and only used for that purpose. Most countries have embedded this principle into their domestic legislation. The national privacy frameworks of the four countries examined establish this provision. Thus, the subsequent automated use of information breaches this principle of international and national privacy regimes. This will be analysed further under the principle of proportionality[59].

[57] Figure elaborated from diagrammatic illustration from Shoniregun, Chalres A., and Crosier, Stephen, *Securing Biometrics Applications* (Springer, 2008) p. 87
[58] For further details, see section 1.4 Hypothesis
[59] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

6.3.7. *Impact on Privacy and Data Protection*. The last major challenge deals with the main impact on privacy and data protection at national and international levels. These concerns are related to privacy and issues of intrusiveness, disclosure, purpose, misuse and consent, among others.

The previous chapter discussed the capacity of biometric systems to obtain an individual's sample without his or her consent[60] and to request additional personal information[61]. It is important to highlight that while not all biometric systems are physically intrusive[62], all biometric systems can undermine privacy and data protection rights.

The intensification and diversification of biometric technology increases privacy concerns nationally and internationally. It is now possible to deliver personal services or online interactions, such as e-Commerce, e-Government, e-Health, e-Education and other electronic activities by means of interactive platforms. While personal data is collected, stored, analysed and exchanged, in most cases, to grant access to multiple electronic identification systems (eID) both on and off the Internet, other cases do so for law enforcement, commercial, social or marketing purposes, or simply for convenience.

These interactive platforms facilitate TBIF by assisting governments in establishing stronger and more accurate identifications[63]. Furthermore, the advances in storage capacity of personal information and the simplification of TBIF create legal concerns

[60] Facial features can be obtained with CCTV and fingerprints, with sensors. Some biometric systems –like fingerprints and facial recognition systems- allow the possibility of unwanted identifications that may imply a risk for the person identified. For example, individuals in witness protection programs may be identified based on their fingerprints or minors may be identified because biometric technology does not make age-related distinctions. Prabhakar, Salil *et. al.,* "Biometric Recognition: Security and Privacy Concerns", (2003) 41 *IEEE Security & Privacy* http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1193209&tag=1 (18/12/2012)

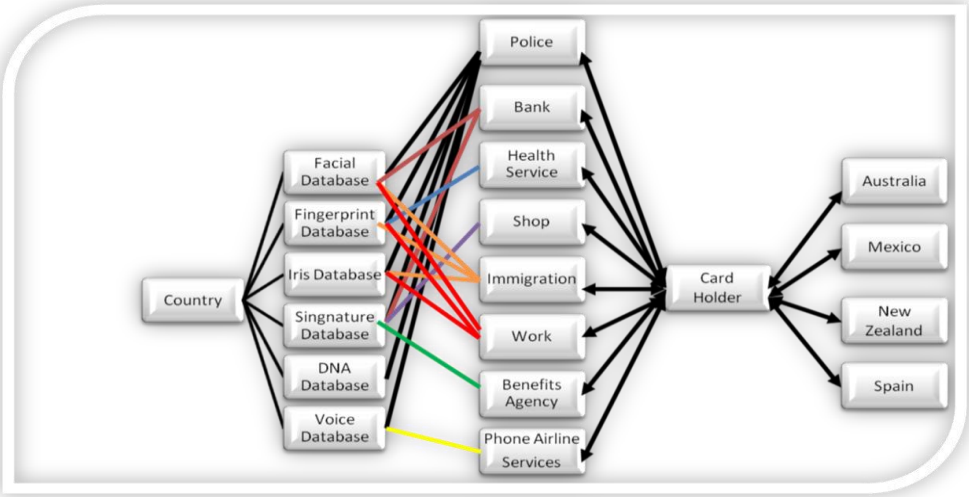
[61] The iris and retina biometric systems may reveal blood pressure and glaucoma. For further details see Chapter 2. Biometric Systems: What is Biometrics?

[62] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

[63] Electronic Identity documents –national ID cards, ePassports, driving licenses and display credit cards, among others- hold one or two biometric data such as a photograph and/or fingerprints. It may incorporate multiple security features to prevent counterfeits, as well as RFID or AIDC technology.

related to the purpose and misuse of information. The figure below shows interactive platforms facilitating TBIF between countries using a unique smart card.

Figure 26. Transborder Biometric Smart Cards[64]



Thus, it is important to enact an adequate privacy and data protection legal framework at national and international levels even though most countries already have provisions governing these privacy and data protection concerns within their borders. An assessment of privacy and data protection legal frameworks will be given in the following chapter[65].

It should be noted that there is, for example, asymmetry in the exercise of the right to access to personal information because this affects personal data protection nationally and internationally. The privacy and data protection legal framework in the four countries examined establish specific procedures for the right to access personal information, however, internationally these procedures are different. These privacy and data protection legal framework also establishes restrictions regarding national security issues and these restrictions prevent privacy commissioners from being able to properly monitor and supervise these databases.

[64] Figure elaborated from diagrammatic illustration from Shoniregun, Chalres A., and Crosier, Stephen, *Securing Biometrics Applications* (Springer, 2008) p. 87.
[65] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

Nationally, two scenarios surface with the exercise of the right to access to personal information: the first scenario is when certain privacy and data protection regimes set a direct procedure to be followed by national agencies when requesting access to personal information. In this case, citizens exercise their right by making their requests directly to the authority or agency. The second scenario is when privacy and data protection regimes set an indirect procedure for requests through a privacy commissioner, an ombudsman or a specific body. This situation means that citizens cannot directly access their information because the request is presented to the privacy commissioner, who then proceeds to request the information from the corresponding agency on the citizen's behalf.

At an international level, some agencies have internal provisions governing the right of access to information. Interpol, for example, has developed internal rules for the protection of the personal data collected and processed by its General Secretariat[66]. The Joint Supervisory Authority of Schengen has developed guidelines for exercising the right of access[67]. Interpol permits any request to be presented directly to the agency whereas with the Schengen, the request is governed by the national regime of the citizen requesting the personal information. The privacy principle of access to personal information, at an international level differs from agency to agency.

Nationally and internationally, the exercise of the right of access to personal information is contradictory and the protection of data is not very user-friendly with all the different procedures and practices.

In summary, seven domestic and global legal challenges can be identified, which pose risks to TBIF. Appropriate models of TBIF should be undertaken with integrity and consistency not only in terms of information, but also in compliance with privacy principle practices. A strict privacy and data protection legal framework is essential to reduce concerns in this area. In addition, a suitable legal regime for TBIF will ensure

[66] *Rules on the Processing of Information for the purposes of international police cooperation (RPI)* (2008); see also, the Supervisory Board for the Control of Interpol's Archives, which was designated to enhance the protection of personal data in the respect for human rights.
[67] Joint Supervisory Authority of Schengen, *The Schengen Information System. A guide for exercising the right of access* (2009) http://www.dutchdpa.nl/downloads_int/Guide_for_exercising_the_right_of_access.pdf (22/12/2012)

effectiveness but more importantly address these national and international challenges. This assessment of privacy and data protection in the four countries is given in the next chapter[68].

6.4. Conclusions

This thesis argued that the deployment of biometric systems and TBIF in both contexts, in immigration information flow and information flow in criminal databases for security reasons raises legal challenges. This chapter has provided an assessment of the central research problem by examining the common legal challenges for TBIF in the contexts of both immigration information flow[69] and information flow in criminal databases[70]. This chapter should not be viewed solely in terms of trying to lay down the results of the research. In contrary, it sets out the common legal challenges of TBIF and their impact to privacy and data protection rights[71]. The chapter assessed old common legal challenges that need to be resolved and identified recent common legal challenges. The subsequent use of biometric information is a new common legal challenge originated by the rapidly developing biometric industry. All these common legal challenges arise at both national and international levels. This is important because the expectation for TBIF in both for immigration control and crime prevention was to find harmonised national integrity and consistency on biometric information and common practices[72].

Jasanoff and Habermas analyse governments and regulations in terms of their differing reception of technology[73], however, these differences occur despite state policies, national priorities, global movements, and the role of key actors.

[68] For further details, see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions
[69] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[70] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow
[71] For further details, see Chapter 1. Transborder Biometric Information Flows: Legal Challenges
[72] For further details, see Chapter 8. Conclusions
[73] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 9, p. 6 and Habermas, Jürgen, “Sfera pubblica (Una voce di enciclopedia)”, above n 12.

Finally, the next chapter discusses privacy and data protection in international and national legal frameworks on TBIF in the four countries examined. While countries examined have some differences in their privacy and data protection legal framework, it is possible to address an adequate regime for TBIF. A strengthened common legal privacy and data protection framework is needed to protect individual rights, as well as to facilitate the TBIF.

CHAPTER 7.

TRANSBORDER BIOMETRIC PRIVACY REGIMES: NATIONAL SOLUTIONS

7.1. Introduction

The preceding chapters examined a rapidly developing industry with a lack of adequate self-regulation[1] and the convergences and asymmetries for TBIF within the four countries study in the contexts of immigration control and crime prevention and the emerging, international regulatory frameworks for TBIF for immigration information flow[2] and for information flow in criminal databases[3]. The thesis has also emphasised the lack of public debate and lack of official information about biometrics[4]. The previous chapter identified the common legal challenges of TBIF in the context of immigration information and information in criminal databases[5].

The four countries study identified two major contexts in which individual privacy and data protection rights may be affected by restricted public interests, namely in the contexts of defence and national security. Restrictions in these two contexts are considered as major concerns for human rights activist and academics who agreed that "governments have increased their coercive powers to detriment privacy and data protection"[6]. Concerns about the restrictions on privacy and data protections in

[1] For further details, see Chapter 3. The Biometric Industry: An illustrative Map of Players, Products and Partnerships

[2] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[3] For further details, see Chapter 5. Biometrics in Criminal Databases: Current Transborder Information Flow

[4] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* (Princeton University Press, 2007) and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Einaudi, 1980).

[5] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges

[6] Interview with Ernesto Villanueva Villanueva and Issa Luna Pla, Professors, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [Legal Research Centre of the National Autonomous University of Mexico] (Mexico City, 23 November 2011); Interview with Charlotte Epstein, Professor, University of Sydney (Sydney, 26 October 2011); Interview with Katina Michael, Associate Professor, University of Wollongong (Sydney, 21 February 2012); Interview with Pilar Nicolas, Professor, University of Deusto (Bilbao, 10 November 2011) and Interview with Lina Ornelas, Instituto Federal de Acceso a la Información y Protección de Datos [Federal Institute for Access to Information and Data Protection] (Mexico City, 15 November, 2011) This component of the

are increasing significantly in the contexts of defence and national security, because of the intensification on the deployment of biometric systems, particularly in TBIF. The justifications for restrictions on individual rights to privacy and data protection frequently refer to common international concerns about threats of terrorism and illegal immigration.

This chapter considers national and international privacy and data protection and recommendations for an achievable legal framework for TBIF and proposes practical and achievable recommendations to address these challenges. These recommendations recognise the emergence of some international organisations in this field. However, these are not official international organisations and their recommendations are not binding. Nevertheless, these international organisations are making valuable contributions to address some of the legal challenges of TBIF, but their recommendations are advisory only and without jurisdiction or authority to address specific domestic problems[7]. Recognising that privacy and data protection operate at national levels, the proposed recommendations acknowledge the adoption of a best practice model must include mechanisms to achieve greater transparency and public accountability within an integrated, a reasonable standardise legal framework.

Importantly, this chapter also discusses the principle of proportionality in relation to the proposed recommendations as a means of balancing the costs and benefits of TBIF and assessing the recommendations themselves. As an analytical and synthetic tool, the “principle of proportionality” enables the assessment of biometric systems in relation to human rights and whether TBIF in immigration control and crime prevention are strictly necessary in a constitutional democratic States. This chapter also assesses international privacy and data protection framework and sets out the current four countries study symmetries, asymmetries and legal gaps in privacy and data protection framework for TBIF. This chapter examines the balance

research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[7] These instances include International Civil Aviation Organization (ICAO), International Organization of Migration (IOM), Asia Pacific Economic Co-operation (APEC), Organization of Economic Co-operation and Development (OECD), Interpol and European Union.

between public and private interests by the Civil Law proportionality test and the Common Law reasonableness standard. Finally, this chapter presents proposals to address the required level of privacy and data protection for TBIF within any jurisdiction.

7.2. International Privacy and Data Protection Regimes

There are no specific international treaties on biometric information flow generally or TBIF in particularly. The emerging international privacy and data protection regime has been developed by a number of organisations that range from regional forums to official regional organisations. On this unofficial to official range are the Asia-Pacific Economic Cooperation (APEC), non-mandatory, Privacy Framework; the Economic Cooperation and Development's (OECD) Privacy and Security Guidelines; the Council of Europe conventions and the mandatory Directives of the European Union on data protection[8].

7.2.1. *The Asia-Pacific Economic Cooperation (APEC) Privacy Framework.* APEC is primarily a forum to promote cooperation in the Asia Pacific region in economic affairs. This regional Asia-Pacific organisation has considered privacy issues in relation to economic cooperation and developed a framework for the constituent members. The APEC Privacy framework is not mandatory or binding on members but may informed policy and legislation for members. The APEC framework is relevant to this thesis, as three of the four countries study are members of APEC.

Importantly, the APEC Privacy framework is a formal advisory but non-binding set of guidelines for members. APEC first considered privacy in 1998, when the APEC issued the *Blueprint for Action on Electronic Commerce*. It was not until 2004 that the APEC group agreed on the *APEC Privacy Framework*; which outlines privacy principles. The 21 member countries may implement these principles in their national legislation, but such implementation is entirely voluntary. Accordingly, the APEC

[8] It is important to note that various countries have created different regional forums to discuss privacy and data protection issues. An example of the importance of these regional forums is the *Resolution on International Enforcement Coordination (2013)* of the annual International Data Protection and Privacy Commissioner´s Conference.

framework is optional and its implementation has not been consistent among member countries[9].

It should be noted that the APEC framework protects cross-border flow of personal information, even outside the APEC region, through the accountability principle[10]. The *APEC Privacy Framework* includes a mechanism for reporting domestic implementation of the framework, guidance for international implementation (information sharing among member economies) and cross-border cooperation in investigation and law enforcement[11]. However, at the time of writing, no report on its implementation was available.

In 2007, APEC issued a pilot programme for the implementation of the privacy framework called, *Data Privacy Pathfinder*[12]. As a result of the Privacy Pathfinder working plan, in 2012, the APEC issued the *Cross-Border Privacy Rules System*, which is a voluntary certification based system[13].

In summary, the *APEC Privacy Framework* is concise, sufficiently general for international implementation and suitably broad for cross-border cooperation for investigations and the enforcement of privacy laws. However, the *APEC Privacy Framework* is not mandatory and requires domestic legislation to be enacted. In addition, the *APEC Privacy Framework* does not impose strict controls and safeguards on privacy and data protection in member countries. It is therefore concluded that the *APEC Privacy Framework* provides a reasonable framework of guidelines, but does not required regulatory implementation or effectiveness on a national level.

---

[9] *APEC Privacy Framework* (2004) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (23/12/2012)
[10] The accountability principle was first established in the OECD Guidelines.
[11] For Australia, Mexico and New Zealand as members of APEC.
[12] The Pathfinder sets objectives for businesses and Privacy Agencies.
[13] *APEC Cross-Border Privacy Rules System* (2012) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx (27/09/2012)

7.2.2. The Economic Cooperation and Development (OECD) Privacy and Security Guidelines. These OECD Privacy guidelines were drafted in 1980 and marked a watershed in the development of personal data protection. Although these guidelines are not mandatory and require national legislation to be implemented, the foundation for the subsequent national privacy and data protection laws of all the member countries. These guidelines were principally concerned with the protection of personal data held by financial organisations and governments within national borders. The guidelines did recognise the international transfer of business and commerce data[14]. At that time, the flow of personal information across national borders increased and thus the protection of personal information flow was considered crucial. The OECD expert group, chaired by Michael Kirby not only focused on the protection of privacy, but also centred its attention on challenges related to cross-border data[15]. These guidelines originally applied for banking and commerce and now have application for cross-border data in general and extended to the emerging concerns about security with the 2002 *Security Guidelines*.

Almost thirty five years ago, the OECD Privacy Guidelines, which are not binding, were the universal foundation and starting point for national privacy and data protections laws. These guidelines encompass eight principles, which are interpreted as the minimum standards that countries should incorporate into their privacy and data protection legislations for TBIF. These eight principles are characterised by flexibility of application: all media, all types of processing and all categories of data -included biometrics-. For our research, three important sections from the OECD Privacy Guidelines are taken into account. The first section is related to the basic principles of international application: free flow and legitimate restrictions. The second section is about national implementation, and the third section is related to international cooperation[16].

[14] Kirby, Michael, "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy" (2010) 20(2) *Journal of Law, Information and Science* 1-14.
[15] Idem.
[16] Idem.

In 2002, the OECD issued Security Guidelines[17], a set of nine high level policy and operational principles that aim to set a minimum level of security for personal information that flows internationally.

It is clear that the OECD Guidelines were a significant achievement and have been an essential basic formula and benchmark for international data protection regulations around the world. However, these OECD Guidelines require direction on how to apply them. Besides, the volume of personal data now being exchanged, collected, retrieved, processed, used and stored cannot compare to the volume of personal data of three decades ago. Thus, it brings up not only the question of whether domestic regimes have been laid down with sufficient precision to protect individuals' private interests against the public interests, but also about the quality of the law in question and the individuals' private interest in the facilitation of linkages of many databases nationally and internationally.

7.2.3. *The OECD and Biometrics Technology*. The OECD continued to consider privacy and data protection on their agenda and consider the development of methods of biometric data. In 2004, the issue of biometric data exchanges was formally considered and the OECD issued a report on biometric recognition technology[18]. In this report, the OECD gave an overview of national policies and legal frameworks, listed international organisations working in the field, identified existing and pilot systems and detected some concerns. These concerns can be classified as pertaining to four areas: first, the potential for encryption; second, the risk that biometric recognition systems can be used for surveillance; third, that the principles of consent and transparency are optional in some implementations and fourth, their susceptibility to security attacks[19].

[17] *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD Council, 1037th sess (25 July 2002) http://www.oecd.org/internet/interneteconomy/15582260.pdf (23/12/2012)
[18] OECD, *Biometric-based Technologies*, Report 101 (2004) http://dx.doi.org/10.1787/232075642747 (22/08/2012)
[19] Idem.

The report recommended that all biometric systems be guided by both the OECD Privacy Guidelines and the Security Guidelines. Moreover, the OECD report also proposed recommendations to the biometric industry in order to ensure that biometric technology complies with privacy and security requirements, as discussed in preceding chapters[20]. The report also highlighted the risks of relying on biometrics as the only security measure, as well as the lack of public independent biometric performance reports.

However, the report did not examine the quality of the domestic laws of their members or require, for example, that the measures implemented to protect personal data should be accessible to the person concerned. It also did not examine whether the law was sufficiently clear in its terms of giving an adequate indication of every circumstance related to cross-border privacy risks or cross-border complaints, in which the authorities are empowered to exchange information with overseas authorities and the procedures to do so.

7.2.4. *The OECD and Cross-Border Privacy Concerns*. The technical cross-linking of data bases prompted the OECD to turn its attention to the increasing rate of TBIF. The OECD formally consider this issue and in 2006 published its *Report on the Cross-Border Enforcement of Privacy Law*[21]. The report shows asymmetries and similarities among 23 member countries and one non-member country in matters of international cross-border data flows, privacy risks and law enforcement co-operation. It turned its attention to domestic privacy law enforcement issues and cross-border aspects of privacy law enforcement. However, it did not provide any solutions to problems related to effective co-operation, cross-border privacy risks and/or cross-border complaints.

[20] For further details, see Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

[21] OECD, *Report on the Cross-Border Enforcement of Privacy Law,* Report 121 (2006) http://dx.doi.org/10.1787/231304814207 (23/12/2012)

The following year, the OECD adopted the *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*.[22] Recently, in 2011, the OECD issued the *Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*[23]. These documents reveal an increase in the number of countries with privacy or data protection legislation and some improvements related to cross-border co-operation done by some privacy agencies. However, the report also recognises that the actual instances of co-operation are still limited[24]. Furthermore, the report did not provide any solutions to the problems of restrictions on sharing information with overseas authorities, cross-border privacy risks or cross-border complaints.

In 2011, the OECD issued a report on a review their guidelines governing the protection of privacy and transborder data flows of personal data[25]. This document identified seven privacy-related challenges and highlighted geographic restrictions on data flows. But once again, it did not provide any solutions or guidance on how to solve these issues.

In summary, the flow of major OECD reports on privacy from 1980 to 2011 confirmed the continuing concerns about individual privacy in the face the technological changes. The more recent reports from 2004 focus on the specific concerns address in this thesis in relation to TBIF in the contexts of immigration and criminal databases. These OECD reports confirm the existence of gaps between the emerging international regulatory framework, like the OECD Privacy and Security Guidelines and the national privacy and data protection laws. These gaps are very apparent in the two contexts of this thesis. Both the OECD Privacy and the Security Guidelines apply to TBIF, but these guidelines have not been generally enacted

[22] *OECD Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007) http://www.oecd.org/internet/interneteconomy/38770483.pdf (23/12/2012)
[23] OECD, *Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, Report 178, (2006) http://dx.doi.org/10.1787/5kgdpm9wg9xs-en (23/12/2012)
[24] Idem.
[25] *OECD Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* (2011) http://dx.doi.org/10.1787/5kg2b7l7pljk-en (23/12/2012)

within national jurisdictions. In addition, there is a practical lack of co-operation in privacy law enforcement within countries and a lack of willingness of privacy and data protection authorities to co-operate with overseas authorities. Both sets of OECD Privacy and Security Guidelines are brief and could apply to all biometric systems in general. However, the OECD Guidelines do not impose sanctions or controls for data protection standards. Nevertheless, both sets of OECD Guidelines can provide a reasonable international framework for standards provided these standards are implemented, with sanctions, at a national level.

7.2.5. *The Council of Europe (CE)*[26] *Data Protection Framework.* Influenced by the work of the OECD the CE, in 1981, developed the first European convention on processing personal data and standards of privacy and data protection: the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (also known as *Convention 108*). The CE is an important regional organisation[27] that is principally concerned with human rights. The CE includes a wider membership of 47 States than the European Union with its 28. In 2001, the CE issued a protocol regarding privacy agencies and transborder data flows[28].

Convention 108 strengths the individual's rights of data protection with regard automatic techniques of processing, storing and exchanging personal data, but concerns arise to what extent national data protection laws afford adequate protection to individuals when data concerning them flow across borders. Therefore, the CE issued an additional protocol to *Convention 108* which recognised that Privacy Commissioners play a critically central role in the effective protection of individuals in cross-border data flows.

[26] An international organisation in Strasbourg which comprises 47 countries of Europe. It was set up to promote democracy and protect human rights and the rule of law in Europe. For further details of legal instruments, see the Council of Europe legal instruments website http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (23/12/2012)

[27] The Council of Europe http://www.coe.int/aboutCoE/index.asp?page=quisommesnous&l=en (23/12/2012)

[28] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1985), as amended by The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, opened for signature 15 June 1995, (entered into force after acceptation by all Parties), as amended by the Protocol to Convention ETS No. 108, opened for signature 8 November 2001, ETS No. 181 (entered into force after acceptation by all Parties).*

Two recommendations and one resolution are particularly significant in *Convention 108*. The recommendations and resolution are non-binding but represent a significant advance in an attempt to create a framework for TBIF in Europe since they address specific issues regarding automated techniques for the storage, use and exchange of personal data and they respond to actual concerns related to privacy and data protection principles. These are: *Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies; Recommendation CM/Rec (2010) 13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling and Resolution (74) 29 related to the protection of individuals vis-à-vis electronic data banks in the public sector.*

- *Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies*[29]*.* This recommendation recognises the increasing trends of automatic data processing, storing and exchanging personal information by public bodies and its exploitation for commercial advantages by the private sector. Therefore, this recommendation establishes Data Protection Principles (DPP) based on the Convention 108 that can be implemented by national legislation to implement these safeguards.

- *Recommendation CM/Rec (2010) 13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling*[30]*.* This Recommendation establishes 13 conditions for the collection and processing of personal data, the rights of data subjects, remedies, data security and supervisory authorities. However, there are exceptions and restrictions are broad and may limit individual privacy. These exceptions are: security, public safety, monetary interests of the State or the prevention and suppression of criminal offences.

[29] *Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies,* adopted 9 September 1991.
[30] *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling,* adopted 23 November 2010.

- *Resolution (74) 29 related to the protection of individuals vis-à-vis electronic data banks in the public sector*[31]*.* This resolution established specific common DPP as a guide to member States to ensure harmonised and uniform implementation of these principles. The aim was to avoid asymmetries between the data protection legislation introduced in the member States.

These CE recommendations and the resolution are not binding unless implemented in national legislation. Nevertheless, these Data Protection Principles have promoted privacy and data protection rights through Europe, in partnership with the European Union (EU). Many members have signed the Convention 108 and implemented it in their respective national legal frameworks.

7.2.6. *European Union and Their Data Protection Legal Framework.* Apart from these three organisations, the European Union (EU) has developed a mandatory regime for privacy and data protection. The EU includes Spain as a member state and is one of the four countries examined in the four countries study. Spain provides an illustration of the mandatory EU legal framework. The EU requires countries dealing with the EU, to comply with their legal framework and can undertake an assessment on the adequacy of a country's privacy standards and remedies[32].

The EU legal framework includes different types of legal documents: conventions, protocols, directives, recommendations and resolutions, all of which are binding for all member countries. However, the most important binding Directives[33] in relation to data protection issued by the EU are the *Directive 95/46/EC*[34] (known as the Data Protection Directive) and the *Directive 2009/136/EC*[35]:

[31] *Resolution (74)29 related to the protection of individuals vis-à-vis electronic data banks,* adopted 20 September 1974.
[32] Article 25.6 EU *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31.
[33] A Directive is a legal act where the EU which normally leave member States a certain amount of leeway to enact rules to be adopted. Folsom, Ralph and Lake, Ralph B. (eds.), *European Union law after Maastricht: a practical guide for lawyers outside the common market* (Kluwer, 1996), p. 5.
[34] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31.
[35] *Directive 2009/136/EC (2009) amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning*

- *Directive 95/46/EC.* On the protection of privacy and data protection this Directive is the main reference text at European level. This Directive applies to data processed and storage in any non-automated and automated databases. Its aim is to set the cross-border regulatory framework balancing the individuals' interests and the public interests for personal data flow in Europe[36].

- *Directive 2009/136/EC*. Amends the actual mandatory EU legal framework for electronic communications networks and services, as well as five directives. These directives embody a breakthrough in regulating personal data processing and the protection of privacy. First, they address a number of issues relating to data processing systems. Second, they were updated after the European Commission (EC)[37] presented its findings on the review of the EU regulatory framework for electronic communications networks and services in 2006[38].

Directive 95/46/EC prohibits the transborder information flow to countries that have inadequate data protection regimes (including European members)[39]. The aim of this prohibition is "to ensure that the cross-border flow of personal data is regulated in a consistent manner"[40]. For the EU, an adequate data protection regime is based on the following requirements:

---

the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, [2009] OJ L 337/11.

[36] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31.

[37] The executive organ of the European Union, based in Brussels, which monitors the proper application of the Union treaties and the decisions of the EU institutions.

[38] *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, on the Review of the EU regulatory framework for electronic communications networks and services,* [2006] COD 2006/334.

[39] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* [1995] OJ L 281/31, article 25(1).

[40] Ibidem, paragraph 8.

a) “Principles of privacy and data protection reflected in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies for processing”[41];

b) “Circumstances under which processing can be carried out; including nature of the data, the purpose, duration of the proposed processing operation, data quality, the rules of law –both general and sectoral- in force in the third country, professional rules, technical security and notification to the supervisory authority”[42];

c) “Rights conferred on individuals; including to be informed of cross-border data flow, to access to the data transferred, to request corrections and to object to the transfer in specific circumstances”[43].

These important Directives have been supplemented with binding recommendations and resolutions specifically applying to biometric systems. However, comparative studies conducted by the EC[44] have indicated that the operational of the privacy and data protection laws within the borders of EU members have asymmetries. Some of the member countries differ in the scope of their implementation of the Directive and in the functions and powers of their privacy agencies. In addition, some academic studies and reports have also highlighted this lack of harmonisation in terms and rules[45].

[41] Ibidem, paragraph 25.
[42] Ibidem, Article 25(2).
[43] Ibidem, paragraph 25.
[44] As it was mentioned earlier the EC is the executive organ of the EU, for further detail above n 38.
[45] Korff, Douwe, “EC Study on Implementation of Data Protection Directive 95/46/EC” (2002). Available at http://ssrn.com/abstract=1287667 (23/12/2012); Bygrave, Lee, “Privacy Protection in a Global Context -A Comparative Overview”, (2004) 47 *Scandinavian Studies in Law* 319-348; Kuner, Christopher, “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future”, *Tilbrug Institute for Law, Technology and Society, (*2010) http://dx.doi.org/10.2139/ssrn.1689483 (23/12/2012); Korff, Douwe, “Comparative Study on Different Approach to New Privacy Challenges, in Particular in the Light of Technological Developments” (2010). http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf (23/12/2012)

The EU legal framework of transborder data facilitates the free flow of personal data among European members. Nevertheless, some challenges may arise when personal information flows out of the European region with different approaches to regulation are applied, because countries outside this region must adjust their national laws to EU legal framework in order to transfer personal data legally.

In summary, in contrast to the APEC Privacy Framework, the OECD Guidelines and the Council of Europe *Convention 108*, the European Union Directives embodies a *mandatory* legal framework. The mandatory EU Directives establishes a regional regime and imposes strict controls and safeguards on data protection. The EU mandatory data protection legal framework extends to countries outside the EU as these countries must have equivalent protections on data protection[46]. The EU legal framework provides a best practice gold standard for the protection of privacy and data protection and ensures regulatory effectiveness at a national level but also for TBIF.

7.3. National Privacy and Data Protection Legal Frameworks: The Four Countries Study

In the absence of a mandatory international privacy regime or binding regional agreements, like the Directives of the EU, privacy and data protection relies on national regulatory regimes. Similarly, TBIF between immigration and criminal databases is primarily regulated by national privacy and data protection laws. The four countries study identified areas of symmetries and asymmetries in the privacy and data protection frameworks in the four countries examined. Before any proposals can be made to better integrate national privacy and data protection regimes, these symmetries and asymmetries must be assessed and their significance balanced. This section focuses on TBIF where data collection and exchanges are carried out by government agencies involved in border control or criminal law enforcement activities.

[46] In Australia for example amendments were introduced to the Privacy Act to comply with the EU, Australia Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol. 1-3.

7.3.1. *Outline of Privacy and Data Protection in The Four Countries Study*. Nationally, the legal framework starts from a constitutional level. Comparative research was undertaken in the four countries study that reveals that the three of the four countries examined, the recognition of privacy or data protection rights starts at this level. Australia is the only country, in the four countries study, that does not have a Bill of Rights. The next level is found in a country's legislation. All four countries have national laws on privacy or data protection.

The Australian *Privacy Act 1988* is the main statute governing privacy at the federal level and has 13 Australian Privacy Principles (IPPs), which apply to federal government agencies and private sector[47]. Meanwhile, in New Zealand, the 1993 *Privacy Act* has 12 privacy principles that govern public and private sectors. Like Australia's Privacy Act, the New Zealand's 1993 *Privacy Act* follows the principles embedded in the OECD Guidelines[48].

Spanish *Organic Law 15/1999 of 13 December on the Protection of Personal Data*[49] embraces not only the OECD Guidelines, but also the EU legal framework. The Mexican legal data protection framework is governed by two piece of legislation, the *Federal Data Protection in Possession by the Private Sector Act*[50] *and* the *Federal Transparency and Access to Governmental Public Information Act*[51]*.* Under the

[47] The Australian Privacy Principles replace both the Information Privacy Principles (IPPs) that applied to government agencies and the National Privacy Principles (NPPs) that applied to some private sector. This new Australian Privacy Principles come into force in March 2014.

[48] The Office of the Federal Privacy Commissioner of Australia stated that Australia's privacy laws and principles "reflect the ideas that have been developed internationally and, in particular, the Organisation for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows or Personal Data (1980).* A growing number of other countries, including New Zealand, Hong Kong, Canada, and many European nations, have also adopted privacy laws". Office of the Privacy Commissioner of Australia, *Guidelines to the National Privacy Principles* (2001) http://www.privacy.gov.au/materials/types/guidelines/view/6582 (23/12/2012)

[49] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, BOE-A-1999-23750 [Organic Law 15/1999 of 13 December, on the Protection of Personal Data] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 (21/12/2012)

[50] *Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares,* DOF 5/07/2010 [Federal Data Protection in Possession by the Private Sector Act] (Mexico) *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf* (21/12/2012)

[51] *Ley Federal de Transparencia y Acceso a la Información Pública,* DOF 11/06/2002 [Federal Transparency and Access to Governmental Public Information last amended on 08/06/12] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf (21/12/2012)

Federal Transparency and Access to Governmental Public Information Act, Mexico regulates personal data in possession by the public sector.

The Mexican *Federal Transparency and Access to Governmental Public Information Act* has one chapter on data protection, which consists of nine articles. It is important to note that since the research for this thesis focuses on legal issues of biometric systems implemented by governments, this legislation is the only significant legislation on data protection in the case of Mexico. For Mexican privacy experts, this kind of regulation raises a number of questions related to the adequate protection of personal data in Mexico[52].

7.3.2. *Symmetries in the Four Countries National Laws.* The research assessment on the four countries study has identified twelve symmetries that may be seen as common strengths in dealing privacy and data protection for TBIF[53]. These symmetries are as follows:

- ✓ The four countries have all developed and published formal privacy guidelines or national privacy principles under powers in their national legislation.

- ✓ The four countries have agencies powers to publish standard codes of conduct for good practices and these must be deposited with the privacy agencies. In Mexico, these are known as guidelines.

- ✓ The four countries have imposed privacy and of data protection obligations on persons, public authorities, enterprises, agencies and other data processing bodies.

[52] Interview with Ernesto Villanueva Villanueva and Issa Luna Pla, Professors, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [Centre for Legal Research of the National Autonomous University of Mexico] above note 11 and Interview with Lina Ornelas, Instituto Federal de Acceso a la Información y Protección de Datos [Federal Institute for Access to Information and Data Protection] This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.

[53] For further details, see Appendix I. Four Countries Privacy Regime (Comparative Table)

- ✓ In the four countries, the formulation of the principles of privacy and data protection have been influenced by the OECD Privacy Guidelines but using different legislative terms in the drafting of their laws.

- ✓ In the four countries examined, the legislative definition includes biometric information within the category of protected personal information.

- ✓ The four countries have revised their domestic law to provide legal remedies for unauthorised access, disclosure or misuse of information. The four countries allow the communication of data between official public authorities under specific conditions.

- ✓ The four countries have provisions for communication of transfers of data between national agencies.

- ✓ Three countries (excluding Mexico) have legislative provisions related to the international transfer and flow of data.

- ✓ The four countries examined all have national privacy agencies (Privacy Commissioners) whose main role is to ensure that the legal data protection framework is enforced.

- ✓ The four national privacy agencies have the following common powers established in their legislation: to investigate breaches under their legislations; review complaints; to approve agency and industry privacy and data guidelines; to review the operation of such guidelines; to supervise, promote, monitor and report privacy and data protection under their jurisdiction; to examine regularly the national legislation and propose amendments to the legislation; to conduct research and studies into privacy and data protection under their jurisdiction; to oversee developments in and to cooperate with

national and international bodies or other governmental agencies dealing with privacy and data protection[54].

- ✓ The four privacy agencies in each country have resources to investigate, review, supervise and monitor public bodies in response to access request in the course of their normal operations.

- ✓ The four privacy agencies have powers to conduct Privacy Impact Assessments (PIA) to examine or measure the privacy risks of any project.

- ✓ Three countries (excluding Spain) have exceptions related to defence and national security in their privacy and data protection laws. The Spanish legislation allows to the Privacy Commissioner to inspect security forces databases.

7.3.3. *Asymmetries in National Laws.* In contrast the research assessment identified seven asymmetries[55] for a common and harmonised TBIF, which are:

- ✓ The New Zealand legislation is the only one that considers "information matching agreements"[56], agreement which allow information matching programmes between agencies through written agreements, which should incorporate the information matching rules.

- ✓ New Zealand legislation is the only one that considers the prohibition of "unique identifiers" as a principle[57].

[54] In the four countries, the privacy and data protection agencies generally have extensive powers to engage in and perform different tasks, from administrative functions to quasi-legislative functions, quasi-judicial functions to enforcement, including the imposition of administrative fines.
[55] For further details, see Appendix I. Four Countries Privacy Regime (Comparative Table)
[56] These information matching agreements sets the specific terms and conditions governing disclosures of personal records, information or data. This specific terms and conditions ensure that the public entity make such disclosures of data and uses such disclosed data in accordance with the requirements of the privacy or data protection law.
[57] Its legislation defines the term "unique identifier" as an "identifier that is assigned to an individual by an agency for the purposes of the operation of the agency; and uniquely identifies that individual in relation to that agency, but does not include an individual's name used to identify that individual". *Privacy Act 1993* (New Zealand), Article 2.

- ✓ The Spanish and Mexican legislation include provisions that databases created or operated by the government[58], must be registered with the relevant Spanish and Mexican privacy agencies.

- ✓ The Spanish legislation is the only one that has special provisions of inspection security force databases.

- ✓ The Spanish and Mexican privacy agencies have powers of inspection of the place of data storage and hardware and software used to process these data whereas in Australian and New Zealand, the privacy agencies have more limited powers.

- ✓ Mexico is the only country where the legislation does not have provisions on the international movement of data. However, the Mexican privacy agency has powers to prohibit the transfer of personal information outside Mexico.

7.3.4. *Gap Analyses: Procedural Barriers for TBIF Harmonisation*. The research in the four countries study revealed four practical and procedural inconsistencies in the area of TBIF. An assessment of these four inconsistencies leads to a conclusion that these are significant barriers against a harmonised and standardised privacy and data protection TBIF framework[59]. The four identified inconsistencies are the following:

1. Three of the four countries in the study have specific legislative provisions related to transborder information flows to countries with equal privacy and data protection laws[60] whereas Mexico the legislative provision is not clear.

[58] The Spanish legislation includes also the private sector. In the case of Mexico the private sector is also included but under the *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* DOF 05/07/2010 [Federal Data Protection for the Private Sector] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (20/12/2012)
[59] For further details, see Appendix I. Four Countries Privacy Regime (Comparative Table)
[60] This term is used generically to mean Common Law Acts in Parliament and in Civil Law the equivalent term is Law. The term “laws” is used by the Inter-American Court of Human Rights and

2. In Australia and New Zealand the method for transborder data is carried out by data exchange requests to specific authorities (known as *ad hoc* or one off request) whereas Spain and Mexico generally have linked national databases to automated international systems (known as systematic data sharing)[61].

3. Spanish law has a "general rule" allowing international transborder of data; however, the Spanish Constitutional Court had made specific ruling two articles in their *Organic Law on the Protection of Data*[62] unconstitutional[63].

4. In all four countries the relevant TBIF legislation does not provide rights to individual access information about personal data transfer or complaints about TBIF to foreign countries.

In relation to the first inconsistency, Australia, New Zealand and Spain apply a strict test and require to which data will transfer to have adequate and equivalent protection. The rationale for this strict test is well articulated in the report by the State Services Commission of New Zealand, namely:

- ✓ The inability to guarantee the protection of personal information in countries without privacy or data protection laws.

---

refers as a: "a legal norm passed by the Legislature and promulgated by the Executive Branch in the manner prescribed by the Constitution or whether, on the other hand, it is used `in the material sense', as a synonym for the entire body of law [Legal System], without regard to the procedure followed in creating such norms and the normative rank assigned to it within the hierarchical order of the particular legal system". Advisory Opinion OC-6/86 (1986) 6 Inter-American Court HR (ser A) at paragraph 15.

[61] For further details, see Chapter 6. Transborder Biometric Information Flow: Legal Challenges.

[62] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, BOE-A-1999-23750 [Organic Law 15/1999 of 13 December, on the Protection of Personal Data] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 (21/12/2012)

[63] The Spanish Constitutional Court ruled these provisions unconstitutional "because they were too broad and could lead to abuse of powers, and failed to meet the principles of accessibility, foreseeability, pressing social necessity and proportionality". *Recurso de Inconstitucional* [Spanish Constitutional Court Complaint Number] 292/2000, 20 November 2000, 4 January 2001) published in BOE. http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf (23/12/2012)

- ✓ Conflicts between different jurisdictions: overseas legislations which come in conflict with national law.

- ✓ The inability of privacy agencies to investigate or enforce the law;

- ✓ The unauthorised release of personal information: possible misuse of information

- ✓ Possible access to data by foreign governments;

- ✓ Overseas judicial decisions that might require the disclosure of data[64];

The second inconsistency is about the method use for transborder data. All four countries have integrated systems that allows cross-checking among of number of national databases, such as immigration, passports, taxation, social services, criminal records, often used to check individuals eligibility for publicly-funded services. However, Australia, New Zealand and Spain have clear legal provisions which permit exchange information or linkage databases for international cooperation to international agencies whereas in Mexico the legal provision is not clear. Nevertheless, the mode in which Australia and New Zealand transfer personal data, including biometric information, is carried out by exchanging specific data from a formal and well detailed request to a specific entity. This type of exchange requires a pre-planned and routine way to share personal information by established rules and procedures. Spain and Mexico have linked their national databases to international automated systems. Generally, in this case Mexico and Spain are connected to international automated systems and can access to all the information storage and share personal data in real time[65]. However, in Spain, the Privacy Commissioner must grant the approval prior the authorisation for the transfer. This type of data sharing raises concerns about inappropriate disclosure of personal data.

[64] New Zealand Government, States Services Commission, *Communication Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management* (2009) at 26.
[65] For further details, see 5.4.3. National Criminal Databases: A Case Study

The Mexican Platform and the Schengen System II (Schengen Zone) are illustrative examples of these international automated systems and linkages of databases[66].

In relation to the third inconsistency the *Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data* had two legal provisions (Articles 21.1 and Articles 24.1 and 2) that were against its Constitution. First, these legal provisions allowed transfers of data between public authorities for purposes other than those for which they collected. Second, that the holder of such data is not informed, when was collected, about the possibility of such a transfer, not being under the rule that creates and regulates the database. Third, the transfer itself is done without the consent of the affected. And that the authorization of such assignments can be contained in a standard range under their organic law[67]. The Spanish Constitutional Court reasoned that rights of those affected to be informed and consent as well as the rights of access, rectification and cancellation, comprise the fundamental right of citizens to control the collection and use of personal data which may possess both public entities and individuals. The consent to transfer personal data is a necessary guarantee of the right to privacy of the individuals, because, without such recognition it would be impossible to control the collection, storage and exchange of personal information requested by governments, so weakening the protection offered to those personal data in the Constitution. And this would happen if public authorities are authorized to organize transfer of personal data without the knowledge and consent of the persons concerned by the Administration standards that are not even established in legislation[68].

The fourth inconsistency is a significant challenge to privacy and data protection in TBIF. There is a little public debate about TBIF and there is little information about how to make complaints as part of individual's rights to privacy and data protection. The right to access information about personal data transfer or complaints about

[66] For further details, see 4.4.3. Regional Organisations

[67] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, BOE-A-1999-23750 [Organic Law 15/1999 of 13 December, on the Protection of Personal Data] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 (21/12/2012)

[68] *Recurso de Inconstitucional* [Spanish Constitutional Court Complaint Number] 292/2000, 20 November 2000, 4 January 2001) published in BOE. http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf (23/12/2012)

TBIF to foreign countries differs in specific terms in each of the countries examined. In Mexico, requests for information for TBIF are accepted by telephone, whereas Australia does not accept the use of telephone. This means that requests have to be in writing. In New Zealand, the Privacy Commissioner cannot consider an information access request from a foreigner unless they are in New Zealand. The New Zealand Privacy Commissioner initially has the power to investigate complaints and attempts to resolve the matter, when the Privacy Commissioner is unable to resolve the issue, the Director of Human Rights (Proceedings0 or the Human Rights Review Tribunal can issue a decision. In Spain, the Data Protection Agency can provide information about TBIF and provides greater protection because of the Spanish Constitutional ruling and the EU framework. The Spanish Data Protection Agency can restrict information for foreign data controllers. By contrast, in Australia, the Privacy Commissioner cannot investigate a foreign data controller. In Mexico and in New Zealand, this situation is unclear.

In summary, considering the emerging international framework for TBIF and the requirement of privacy and data protection, TBIF requires a harmonised and standardised privacy and data protection framework. This thesis acknowledges the foundational importance of the OECD Guidelines and their influence in the development of the international framework for privacy and data protection. The research assessment in the four countries study demonstrates that the national standards for privacy and data protection should be extended to TBIF. However, there are critical inconsistencies in areas such as law enforcement, privacy risks for TBIF and limited co-operation among privacy agencies. However, the similarities between these four countries are more significant than the asymmetries. Overall, the gap analysis revealed some procedural barriers in relation to TBIF, particularly in relation to individual information and complaints in relation to TBIF. These procedural barriers affect negatively individual privacy and data protection rights. Therefore, national legislation must address the TBIF in a standardised and harmonised fashion as proposed in this chapter[69].

[69] For further details, see section 7.6. Options for a Common Framework for Transborder Biometric Information Flow

7.4. The Principle of Proportionality: Legitimate Restrictions on Privacy and Data Protection

Rights to privacy and data protection are not absolute rights and may be qualified by restrictions that are reasonably justified. This section considers the necessary balance of public and private interests and the measures that may be reasonable to justify restrictions on individual privacy and data protection for the protection of public interests. This section examines how and to what extent the Civil Law principle of proportionality and the partner Common Law standard of reasonableness can be applied to address the balance between individual privacy and data protection and public interests, such as national security and defence. These exceptions work as restrictions on or interference with privacy and data protection rights. This balance was apparent in the four countries study in which Spain and Mexico apply the proportionality test and Australia and New Zealand the reasonableness standard.

7.4.1. *The Principle of Proportionality*. There are general principles of law, in Civilian Law countries and in European Law countries, which are applied by national courts when determines the lawfulness of legislative and administrative measures. These general principles are proportionality, legal certainty and legitimate expectations[70]. These general principles are used as a control over the exercise discretionary powers of public authorities. The principle of legal certainty balances the consistent relationship of legislation to the surrounding legal system and its rational justification. The principle of legitimate expectations balances the public interest and the behaviour of authorities in the light of the actual circumstances of a particular case. The principle of proportionality is concerned with balancing of public and private interests[71].

[70] General principles of law should be distinguished from rules of law as principles are more general and open-ended in the sense that they need to be honed to be applied to specific cases with correct results. Thomas, Robert, *Legitimate Expectations and Proportionality in Administrative Law,* (Hart Publishing, 2000).
[71] Idem.

The principle of proportionality must be derived from a legal bases and be "necessary or reasonable limits that can be demonstrably justified in a democratic society"[72]. Accordingly, a strict justification for an interference with individual privacy or data protection must be necessary and legally justified in a democratic society. The principle of proportionality is found in most Civil Law tradition systems. From its German origins, it spread across Europe and Latin America, but also to some Common Law systems like England, Canada, New Zealand and mixed systems like South Africa[73]. In addition, this principle is also applied by the European Court of Human Rights[74] and the Inter-American Court of Human Rights[75].

7.4.2. *The Reasonableness Standard.* The reasonableness standard applies in Common Law countries but still there are some questions about its formal recognition of this standard and its equivalency to the proportionality principle. Michaelsen argues that "Australia still awaits formal recognition [of reasonableness] in constitutional law and administrative law"[76]. On the other hand, Downes accepts the relationship of reasonableness and proportionality in Australia[77] and points to the lack of adoption of the principle of proportionality[78]. Canada has formally recognised the proportionality test and that test has been applied by the Supreme Court[79]. It has been referred to as the "Oakes test"[80]. This test has replaced by the "reasonableness standard". In 2012, the Supreme Court of Canada considered that an administrative action which affected human rights should be assessed by the Oakes test. In the

[72] Nicholas, Emiliou, *The Principle of Proportionality in European Law: A Comparative Study,* (Kluwer Law International, 1996); Sanchez Gil, Ruben, *El Principio de Proporcionalidad*, (UNAM, 2007).
[73] Nicholas, Emiliou, *The principle of proportionality in European law: A comparative study,* above n 73.
[74] For information on the European Court of Human Rights http://www.echr.coe.int/ECHR/homepage_en (23/12/2012)
[75] For information related to the Inter-American Court of Human Rights see http://www.corteidh.or.cr/index.cfm?&CFID=1489195&CFTOKEN=37930864 (23/12/2012)
[76] Michaelsen, Christopher, "The Proportionality Principle, Counter-terrorism Laws and Human Rights: A German-Australian Comparison", (2010) *Berkeley Electronic Press,* 2:1. http://law.bepress.com/cgi/viewcontent.cgi?article=1230&context=unswwps-flrps10 (23/12/2012)
[77] *South Australia v Tanner (1989) 166 CLR 161 and Australian Broadcasting Tribunal v Bond (1990) 170 CLR 321*.
[78] Downes, Garry, "The relationship between reasonableness, proportionality and merits reviews in Australia", (Paper presented at New South Wales Young Lawyers Seminar Issues of Administrative Law, Sydney, 24 September 2008).
[79] Dieter, Grimm "Proportionality in Canadian and German Constitutional Jurisprudence" (2007) 57 (2) *University of Toronto Law Journal* 383-397.
[80] *R v Oakes*, [1986] 1 SCR 103.

later *Dore* case[81], the Canadian Supreme Court acknowledged the difficulty of applying the *Oakes* test in an immigration context, where it is often an administrative process rather than a formal court/tribunal proceeding.

In the two contexts of immigration control and crime prevention data exchanges, individual rights privacy and data protection frequently collide with public interests in national security and defence. The principle of proportionality and the Common Law reasonableness can determine, in specific cases, the State's rights to restrict individual rights providing reasonably justified restrictions in a democratic society. The principle of proportionality defines the legal limits to individual rights[82].

In summary, biometric systems deployed in the two contexts of immigration control and crime prevention are not all physically intrusive[83], however, all may undermine privacy and data protection rights, in some cases. National and international exchanges of personal information should be for specific purposes and those purposes justified. In addition, this TBIF and subsequent use of biometric information raise legal challenges, and the question arises whether this flow of information is reasonably necessary in a democratic society under the proportionality standard[84].

7.4.3. *Applying the Principle of Proportionality: in International Courts*. The proportionality test has not been only applied in national courts but also in international courts. In the Argentinean case, the Inter-American Court of Human Rights has decided that the solution to the conflict between human rights and public interest "requires examining each case in accordance with its specific characteristics and circumstances, considering the existence of elements and the extent thereof on which the consideration regarding proportionality are to be based"[85].

[81] *D v Barraeu du Quebec*, [2012] SCC 12.
[82] Tor-Inge, Harbo, "The function of the Proportionality Principle in EU Law" (2010) 6(2) *European Law Journal* 158-185.
[83] For further details, see Chapter 2. Biometrics Systems: What is Biometrics?
[84] For further details, see section 1.4 Hypothesis
[85] *Kimel v. Argentina (2008) 177 Inter-American Court HR (ser C)* at paragraph 51.

Similarly, the European Court of Human Rights (ECHR) in considering the proportionality test takes account of the "particular context in which information is obtained and stored, the nature of the information and the way in which it is used"[86]. The ECHR has emphasised the importance of an individual's enjoyment of the right to respect for private and family life[87]. The features of a private life include privacy of communications, security and privacy of mail, telephone, email and other forms of communication. These features include the privacy of access to databases. The ECHR has also held that the legal concept of private life includes elements related to an individual's right to his or her own image[88] and an individual's voice[89]. This is an important decision in relation to the storage of biometric face images and voice recognition systems deployed in immigration control and criminal databases. In relation to data storage, the ECHR has stated "the State has a positive obligation to ensure an effective deterrent against grave acts to an individual's personal data sometimes by means of efficient criminal law provisions"[90].

In other cases, however, the ECHR has recognises the power of law enforcement authorities to restrict individuals' right regarding the compiling, storing, using and disclosing of personal information in a police file[91]. The subsequent use of stored information is allowed in accordance of the law and is necessary in a democratic society to achieve the legitimate aims of national security and public safety[92]. These cases demonstrate that the public purpose, use and deployment of biometric information in TBIF require an application of this test to decide whether privacy and data protection measures introduced are necessary and justified in a democratic society.

---

[86] *Peck v the United Kingdom (2003) 36 EHRR 41, EMLR 287.*
[87] *Marper v. The United Kingdom (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008)* at paragraph 41.
[88] *Sciacca v. Italy (European Court of Human Rights, Application No 50774/99, 11 January 2005)* at paragraph 29.
[89] *P.G. and J.H. v. The United Kingdom (European Court of Human Rights, Application No 44787/98, 25 September 2001)* at paragraph 59-60.
[90] *X and Y v. The Netherlands (1985) 91 Eur Court (ser A)* at paragraph 23-24 and 27.
[91] Leander v. Sweden (1987) 116 Eur Court (ser A) at paragraph 48.
[92] *Amann v. Switzelard (European Court of Human Rights, Grand Chamber, Application No 27798/95, 16 February 2000)* at paragraph 69.

The ECHR assesses restrictions put in place for reasons of national security and public safety to decide whether measures go beyond what is strictly necessary. In this regard the ECHR accepts that "domestic legislature enjoys discretion, and it is not for the Court to substitute their assessment for those of national authorities. Nevertheless, the ECHR has stressed that this does not mean that the Contracting States enjoy an unlimited discretion to subject citizens within their jurisdiction to secret surveillance. The ECHR recognizes the danger of restrictive laws undermining or even destroying democracy on the ground of defending it. The ECHR has stated that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate"[93]. The ECHR also held that "the protection afforded by article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private life interests"[94]. Finally, the ECHR has also recognises that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life"[95].

In summary, the European Court of Human Rights (ECHR) has been applying the proportionality test in different cases and has recognised different elements for privacy and data protection rights. In balancing private and public interests, the ECHR has considered, on the one hand, the dangers of the extensive use of biometric systems against individuals' rights, but on the other hand the potential benefits, such as national security and public safety. The ECHR recognises that biometric systems *infringe* privacy and data protection rights. But, the implementation is *necessary in a democratic society* and has to be *in accordance with the law.* Every measure, policy or legislation that may affect privacy and data protection must be balanced by this proportionality test or reasonableness standard. This balance of public and private interests diminishes legal concerns about

[93] *Klass and Other v. Germany, (1978) 214 Eur Court HR (ser A)* at 49.
[94] *Amann v. Switzelard (European Court of Human Rights, Grand Chamber, Application No 27798/95, 16 February 2000)* at paragraph 69.
[95] *Valenzuela v. Spain (1998) Eur Court HR.*

restrictions imposed in the context of defence and national security especially with biometric technology deployed to individuals, but more importantly the use of this proportionality test can be interpreted as being in itself sufficient to secure legitimate decisions[96].

7.4.4. *Applying the Proportionality Test: in Public Policy*. Recognising that the principle of proportionality is a legal test for managing specific disputes on privacy and data protection, balancing public and private interests, the principle of proportionality may also apply at the governmental policy level in the deployment and expansion of biometric surveillance in general and in TBIF in particular. In this respect the proportionality test can be used as a public policy tool but can also be used in more open public debates about the technology to support the justification of the deployment of biometric surveillance in TBIF. Nevertheless, there is a limit to this interpretation determined by the proposed function of the principle. The application of this principle can move beyond the courts of law to be used in the public arena for public purposes in debates about the use and deployment of biometric information in TBIF. The principle can test the justification, proportionality and balance between an individuals' privacy and data protection rights and a state's public interests.

To apply the proportionality principle in the policy context, the following three requirements in a legal dispute must be fulfilled; these same requirements should apply in public policy for the introduction of any restriction of individuals' privacy and data protection rights:

Adequacy. The measure adopted by the government must be rationally related to publish policy aims and the interference should restrict the right or freedom in question as little as possible. In this case, the measure adopted is the public purposes, use and deployment of biometric information in TBIF while privacy and data protection are the associated rights in question.

[96] Habermas, Jürgen, *Between Facts and Norms* (MIT Press, 1998), 259.

Necessity. The measure should be necessary for the legitimate aim for which the measure was introduced. For the purposes of this thesis, the measures introduced should relate to the prevention of illegal immigration and the prevention of crime and terrorism.

Proportionality. This third essential requirement is the balancing of competing privacy and public interests. This analysis includes an assessment of balance between costs and benefits[97]; taking into consideration the following elements in order to identify whether a measure is disproportionate or reasonable[98]:

A. An examination of whether relevant and sufficient reasons have been advanced in support of the measure being pursued[99].

B. An examination of whether there are any less restrictive alternatives and the justifications for no introducing less restrictions options.

C. An examination or whether the interference is "in accordance with the law"[100], which means is permitted in national law.

The proportionality test can be applied to the specific example of biometric passports, as a biometric system deployed in the context of immigration control. Biometric passports are not the only security measures deployed to stop illegal immigrants and prevent terrorism[101]; there are also improved other passenger identification systems introduced to certify the identification of individuals entering at

[97] The Spanish Constitutional Court has stated that "Pondered or balanced because more benefits or advantages for the general interest are derived from it than damages against other goods or values in conflict". *Sentencia Tribunal Constitucional* [Constitutional Tribunal Sentence], 66/1995, 8 May 1995, 13 June 1995 published in BOE. http://www.boe.es/buscar/doc.php?coleccion=tc&id=SENTENCIA-1995-0066.
[98] Michaelsen, Christopher, "The Proportionality Principle, Counter-terrorism Laws and Human Rights: A German-Australian Comparison", above n 76.
[99] As elsewhere argued in this thesis the reasons advance to be openly and public debated or at least these reason publicly available. Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.
[100] This is the common formula.
[101] For further details, see subsection 3.3.2. ePassport Technology: The New Generation

border controls[102]. According to Habermas, in cases where the proportionality test is applied in a strong rights regime, the structure of the court's reasoning is, in itself sufficient to legitimise its decision[103]. However, the proportionality principle should be viewed as a tool for reinforcing privacy and data protection rights and not as simple balancing exercise between a legislative act and an argument of policy. Otherwise, the court may decide in favour of the legislators or the policy makers. The implementation of biometric systems in immigration control cannot, however, prevent all threats of terrorism. Interpol recognises that the documents used to issue a passport (usually fake birth certificates) may be forgeries enabling terrorists to travel with valid biometric passports[104].

7.5. Recommendations to Address Legal Framework for TBIF

It is acknowledge that international organisations are developing international privacy and data protection frameworks, which are broad, brief, but not binding. These frameworks require domestic legislation to be enacted. The thesis considers that the best practice standardised TBIF model is the regional, but official EU data protection legal framework. The EU Directives are mandatory but leave member States a certain amount of leeway to enact their own laws and rules to be adopted. The research assessment on the four countries study revealed common strengths and asymmetries, but also identified procedural gaps. While the asymmetries between the four countries examined are not significant, the procedural gaps create significant challenges for a common and harmonised privacy and data protection framework for TBIF. The proportionality (reasonableness) principle balances public interests and individuals' privacy and data protection rights, and this thesis confirms its value on assess biometric systems and TBIF, which must be strictly scrutinised, supervised and regulated in accordance with the law. However, to address the challenge of procedural gaps in the four countries study the thesis proposes some recommendations for a harmonised and uniform TBIF.

---

[102] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[103] Habermas, Jürgen, *Between Facts and Norms,* above n 96, p. 259.

[104] Darwish, Jamil "International efforts against currency & security document counterfeiting" (Paper presented at the Tenth ID World International Congress, Milan, 3 November 2011) Darwish is an Interpol member staff.

7.5.1. *Options for addressing TBIF Challenges.* Recognising that within an emerging international privacy and data protection framework and the gaps for TBIF, the main solution proposed acknowledges that amendments to privacy and data protection laws is the preferred regulatory pathway. Reinforcement of the existing privacy and data protection laws is preferred over creating new specialised legislation or a specific part on biometric information in existing legislation. The aim of these recommendations is to reduce legal challenges. It is possible; however, that data security and possible misuse of biometric information will remain as privacy risks.

Three possible options may be proposed to address the identified TBIF challenges in immigration and criminal databases. The preferred option should provide practical and achievable solutions and provide a common and uniform legal framework for TBIF in order to achieve an adequate and proportional level of protection. The three proposed options are: first, reinforcement of privacy and data protection laws; secondly, the introduction of a specialised legislation; and, thirdly introduction of specific biometrics provisions by amendment existing legislation.

Option One: Reinforcement of privacy and data protection laws.

The first option proposes to reinforce existing privacy and data protection laws[105]. This option will require harmonisation by reinforcement of the existing privacy and data protection laws in seven areas:

a) *Registry of filing systems.* To achieve transparency and accountability regarding biometric databases should be registered. The registration of biometric filing systems or processing of biometric information in the public sector should be under the jurisdiction of the Privacy Commissioner Agencies. Border control

[105] This term is used generically to mean Common Law Acts in Parliament and in Civil Law the equivalent term is Law. For further details, see above note 60.

agencies and police forces should be included in the list of data controllers. This type of registration is operating in Spain and Mexico[106].

b) *Co-operation with other data protection agencies*. Privacy Commissioner Agencies should perform their functions with clear and effective mechanisms for collaborating with overseas equivalent privacy or data protection agencies in order to ensure a continuity the legal level of individuals' protection across borders. The individual rights to protection personal data should extend to individual's right to access their information where the information is held overseas[107]. This right should include the capacity for an individual to make cross-border: enquiries[108], objections, and complaints. This would create a proportional balance between citizens and government.

c) *Citizens Guidelines for TBIF.* Privacy Commissioner Agencies, in collaboration with police and border control agencies, should develop citizens' guidelines regarding individual rights in TBIF in the two contexts of immigration and criminal databases[109].

d) *Access electronically to information*. In this computer age of electronic communication, individuals should have access to their personal information by means of electronic requests. This electronic access to the specific authorised data holder should include transborder authorities. In Mexico, a request for access to information is permitted by phone or any other electronic forms to applicants in country and overseas[110].

[106] As a further example The Slovak Republic the obligation to register filing system is operating under the Office of the Personal Protection http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=558 (19/03/2014)
[107] It is important that individuals know who is the public entity that will answer the request is and in case this entity is the wrong one, this entity should assist to address the correct one.
[108] It is important that individuals know how to do a request for accessing personal data. This request should be address without any formalities, it is suggested to keep it simple.
[109] In addition, these entities should develop for the protection of minors specific public policy plans for TBIF in these two contexts which to include access on the minor behalf.
[110] *Ley Federal de Transparencia y Acceso a la Información Pública,* DOF 11/06/2002 [Federal Transparency and Access to Governmental Public Information last amended on 08/06/12] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf (21/12/2012)

e) *Codes of conduct for TBIF.* Privacy Commissioner Agencies in collaboration with police and border control agencies should develop codes of conduct applying to border control data officers' by encouraging more respect for individuals' rights in relation to TBIF provisions.

f) *Transborder Data Protection Agreements*. The regulation of transborder data protection should extend to other countries[111] to which the data is transfered. Transfers to other countries should be managed through "information matching agreements"[112]. This is the case in New Zealand, which allows information matching programmes between agencies through written agreements.

g) *Definition of "personal data".* Currently the definition of "personal data" varies in legislation in different countries. In some countries privacy or data protection legislation, the term "personal data" means any general information about or relating to the individual who, is or can be identified, either from the data or from the data in conjunction with other information (that is in or is to come into the possession of the data controller)[113]. In this definition, biometric information is included. But in other legislation, the definition of privacy or data protection describes the specific type of information, such as physical, physiological, mental, economic, cultural, social, genomic identity, among others. In this case, the omission of biometric information as personal data is critical and it must be included by amendment.

This series of amendment proposals for existing privacy and data protection laws is the preferred option to produce and achievable solution for a common and uniform legal framework for TBIF. This "reinforcement option" is informed by the research findings of the four countries study. It is the preferred model and is designed to achieve a best practice model for common TBIF. This "reinforcement option"

[111] The transfer of personal data to another country may include transfer to another country for further processing and as such there must be guarantees of adequate levels of protection to ensure that the rights of individuals are safeguarded in these countries.
[112] These information matching agreements set the specific terms and conditions governing disclosures of personal records, information or data. This specific terms and conditions ensure that the public entity make such disclosures of data and uses such disclosed data in accordance with the requirements of the privacy or data protection law.
[113] Generally, the data controller is who controls the contents and use of personal data.

considers the identified asymmetries in the gap analysis. The adoption of the recommendations, set out above not only achieves a harmonised framework for TBIF, but also addresses the required level of operational effectiveness.

Option two: Specialised Legislation.

The second option recommendation is to draft specialised biometric data legislation. This option was undertaken in the states of New Jersey and Illinois, USA. In 2002, the state of New Jersey introduced the *Biometric Identifier Privacy Act (A-2448)*[114] and in 2008, the state of Illinois introduced the *Biometric Information Privacy Act (740 ILCS 14/1) (2008)*[115]. Both Acts are brief and introduce rights of action for cases of violations of individuals' biometrics privacy through the courts[116]. However, it is not recommended that similar specialised legislation should be introduced[117]. First, the legislative processes in different countries cannot guarantee a uniform act would be introduced, without a common policy approach. This is politically unlikely and, in any case the legislative processes are protracted. Secondly, specialised legislation may require a specialised agency or authority with specific powers and functions. This new biometric privacy and data protection authority would be difficult to establish without guarantees of consistent staffing, levels of funding and powers of inspection. This new biometric privacy authority would represent increased bureaucracy at the time of political commitment to smaller government and with smaller spending on public funds. Thirdly, specialised legislation is problematic in federal jurisdictions, where state level legislatures may have power to legislate in privacy. It is possible that in this system local legislators have differences with other local legislators and federal legislators.

[114] For full content of New Jersey legislation see Appendix K. Legislation of Biometric Identifier Privacy, New Jersey

[115] For full content of Illinois legislation see Appendix L. Legislation of Biometric Information Privacy, Illinois

[116] At the time of writing some academic articles were found, however, these articles only mention the existence of these legislation, but it is unclear how these legislation has been working. No cases were found. The only available information are websites of legal firms and blogs.

[117] For further details, see section 7.3. National Privacy and Data Protection Legal Frameworks: The Four Countries Study

Option three: Amendment of existing legislation.

A third option is to amend an existing Act to include a specific Part or Division on Biometrics. That was the approach taken in the *Works Act-Statutes 1997* of Ontario, Canada[118]. This amendment is brief and generalised, and enacted the provisions of the *Freedom of Information and Protection of Privacy Act* to apply specifically to the *Works Act 1997*. This is a unique approach in one Province of Canada and is not recommended as a general approach to the regulation of biometrics. The thesis does not propose to include a specific section on biometrics in terms similar to the *Works Act 1997*.

7.5.2. *Practical and Achievable Solution: Option one.* This thesis argues and concludes that the best model for achieving a harmonised, common and uniform TBIF legal framework is the first option. The recommendations of this first option will provide integrity and consistency in TBIF practices, both nationally and internationally. The other two options do not guarantee effectiveness and would not reduce the identified legal challenges.

Most importantly, the legislative process in some countries is complicated and lengthy for introduction of the initiative for any formal enactment of a new law. For this reason, it is argued that option one, to reinforce privacy and data protection laws than drafting new specialisation, is recommended as the most practical and achievable option. In addition, reinforcing the administrative supervisory role of national Privacy Commissioners is equally more viable, practical and achievable solution for a common TBIF legal framework at a national and international level.

7.5.3. *Implementation of Option One in National Legislation*. The implementation of the preferred option one can be achieved by amendment to privacy and data protection legislation. In three of the four countries studied it is recommended that the reinforcement option can be achieve by amendments of their privacy and data protection legislation. For Mexico, it is recommended that amendment consist in a

[118] For full content of Ontario biometric information section, see Appendix M. Legislation of Ontario, Canada

new section on TBIF be inserted into the Mexican *Federal Transparency and Access to Governmental Public Information*[119].

The seven proposals set out above at 7.5.1 are not all essential elements for a complete package of reforms for implementation[120]. Option one can be achieved by translating the first three proposals into practice as the minimum level requirements for this initiative at a national level. These three proposals of the seven are critical also for the harmonisation of TBIF at the international level. The final four proposals are desirable but not essential requirements[121]. The following three main areas must be implemented:

a) The registration of biometric filing systems or processing of biometric information of the public sector, including border control agencies and police forces databases.

This may be ambitious but will reinforce the role of the privacy and data protection agencies. Registration is required under the respective jurisdictions of national privacy and data protection agencies. Privacy and data protection agencies are the appropriate and capable agencies to monitor and supervise the management and operation of biometric databases[122]. In addition, reinforcement will enable scrutiny of

[119] Mexican data protection regime is divided in two laws, one for the public sector through the *Federal Transparency and Access to Governmental Public Information* and another for the private sector. This thesis only focuses on the data protection for public sector. *Ley Federal de Transparencia y Acceso a la Información Pública,* DOF 11/06/2002 [Federal Transparency and Access to Governmental Public Information last amended on 08/06/12] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf (21/12/2012)

[120] For further details, see section 7.5.1. Options for Addressing TBIF Challenges.

[121] The four proposals not required are: d), e), f), and g). The proposal d) related to the access electronically to information is incorporated as part of proposals a) and c). While the proposal e) about codes of conducts may continue working with the actual powers of Privacy and Data Protection Agencies to supervise in combination with the promotion of individuals' rights in TBIF. The proposal f) the development for information matching agreements for transfer data to other countries may continue working with the current flow of information framework between national entities where Privacy Commissioners Agencies have powers to supervise. Finally, the proposal g) regarding the inclusion of biometric information in the definition of "personal data" can be left to Privacy or Data Protection Authorities interpretation by an individuals' request, queries, complaints or advisory opinions.

[122] As elsewhere argued in this thesis the reasons advance to be openly and public debated or at least these reason publicly available. Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 4 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 4.

the actual number of biometric databases, the authorities acting as data controllers and individual access electronically to personal information.

b) Cross-border co-operation with other data protection agencies through agreements.

Privacy and data protection agencies must work together to establish a harmonised and consistent framework for TBIF. International co-operation agreements must encourage practical co-operation and willingness to develop effective mechanisms for ensuring the legal continuity level of protection in TBIF. These cross-border co-operation agreements must also include an assessment of performance of cross-border priorities; identification of areas for further improvements; and, promotion of individual rights internationally within this cross-border agenda.

c) Promotion of individuals' rights for TBIF in a cross-border agenda.

Privacy and data protection agencies have the obligation to review and promote privacy and data protection rights. Within this promotion role, privacy and data protection agencies should develop citizen guidelines on individual rights in TBIF. These guidelines should include rights to access electronically to their information; make electronic cross-border objections; enquires; and, complaints. The inclusion of these rights will increase not only trust between citizens and governments, but also will help to scrutinise biometric databases[123].

In summary, reinforcing these three main areas of supervisory powers of privacy and data protection agencies is practical and achievable for TBIF. In addition, this reinforcement approach empowers privacy and data protection agencies in an active and proactive involvement to establish a harmonised and consistent TBIF framework. The implementation of option one is consistent with the proportionality test and addresses the procedural gaps in the four countries study. However, it does not guarantee data security and avoidance of possible misuse of biometric information.

[123] Idem.

7.6. Conclusions

This chapter identified a broad and non-mandatory TBIF framework which relies on practical lack of co-operation and a lack of willingness in privacy and data protection international agreements. In addition, the comparative research revealed legal similarities, asymmetries and procedural gaps in the current operational legal privacy and data protection legislation for TBIF. These legal asymmetries and procedural gaps in combination with the proportionality and reasonableness tests are used to develop three options as a recommendation for addressing a balanced, common and harmonised legal framework for TBIF in a general context.

The chapter presented the principle of proportionality (reasonableness) in international courts and in the public policy arena with the aim of maintaining a proper balance between private and public interests. According to the cases in which the proportionality test was applied by the European Court of Human Rights, the implementation of biometric systems and TBIF for immigration control and crime prevention purposes directly affects privacy and data protection rights.

Recognising the biometric industry's indifference toward becoming self-regulated, combined with poor scrutiny and a lack of public debate has created a fragile environment for the protection of civil liberties, in privacy and data protection. These factors increase the risk of an adequate level of TBIF protection in the two contexts, of immigration control and crime prevention[124]. The proposed recommendations related to the reinforcement of privacy and data protection agencies is the only viable, practical and achievable solution for a proportionate and harmonised TBIF regime.

The main recommendations offer practicality and achievability for overall effectiveness in legal protection in the TBIF environment, in which the amount of information collected, stored and exchanged is increasing globally.

[124] For further details, see Chapter 8. Conclusions

CHAPTER 8.

CONCLUSIONS

8.1. Overview of Transborder Biometric Information Flow: the Area of Study

Information and Communication Technologies (ICT) generally pose different legal challenges and, foremost among these challenges are privacy and data protection concerns related to collection, storage and exchange of personal information. Biometric databases are measures, which have been implemented by many countries for security reasons. This thesis has analysed privacy and data protection challenges to civil liberties in the specific context of ICT in relation to Transborder Biometric Information Flow (TBIF). The thesis analysed TBIF in two specific contexts of transborder exchanges, namely immigration information flow and information flow in criminal databases. This thesis did not analyse the technical aspects or performance of biometric systems nor political reasons for their introduction. Rather, this thesis focused on the legal challenges posed by TBIF and its impact on privacy and data protection rights and civil liberties in these two specific contexts. In this regard, the thesis has evaluated the current limited national and international regulation of the legal framework for the TBIF and assessed how far restrictions on privacy and data protection in these two specific contexts are justifiably proportional and reasonable[1].

The thesis outlined the ICT industry and its development of a range of biometric identification, verification and exchange systems for personal biometric information. The thesis proposes that the biometric industry itself and the responsible government agencies have failed to adequately address concerns about privacy and data protection. To address this gap a model is proposed to achieve a best practice harmonised common TBIF legal framework to reinforce the regulation of TBIF at a

[1] See Chapter 1. Transborder Biometric Information Flows: Legal Challenges

national level. This will model provide integrity and consistency to information flow and common practices both nationally and internationally[2].

This concluding chapter draws together the findings and conclusions of the thesis. First this chapter sets out the significance of TBIF and the general lack of public debate about the rapid and continuing deployment of this biometric technology. Research was undertaken principally by website searches to develop a general map of the industry[3]. This research revealed an expanding industry in terms of its technical capacities and ingenuity but one that has been little concerned with regulatory issues and has done little towards establishing a satisfactory self-regulation framework. Secondly, the thesis examined the emerging international regulatory framework and its limitations and identified the primary reliance of privacy and data protection regimes for TBIF at a national level. Thirdly, in TBIF in the two specific contexts of immigration information flow and information flow in criminal databases, the thesis revealed significant gaps and asymmetries in national collection, storage and exchange of personal information in national privacy or data protection laws and the emerging international regulation framework. Finally, the thesis presents three proposals for practical and achievable national approaches to address TBIF challenges within existing national privacy and data protection frameworks. Throughout the thesis, the arguments for privacy and data protection reinforcement are accompanied by political and social science arguments for greater transparency, scrutiny and public debate about the operation and impact of this technology. This theme of the necessity of informed public debate accompanying and keeping pace with rapid developments in ICT, was a central theme of this thesis.

8.2. Significance of the study: the for Public Debate and Regulation

The thesis argued that there are significant legal challenges involved with ICT but particularly problems with TBIF in the specific contexts of immigration information flow and information flow in criminal databases. Whilst TBIF has been studied from

[2] See section 7.5. Recommendations to Address Legal Framework for TBIF noting that other options were discussed.
[3] Noting the absence of traditional referred publication in this area.

a technical perspective, there is a significant absence of any substantive and critical legal literature. The technical aspects of biometrics have been discussed in the publicly available literature but, this technical literature not been scrutinised by social scientists. This has led to a lack of interdisciplinary studies on the social and ethical dimensions and challenges of the new biometric systems[4].

From the outset of this thesis, and noted throughout, not only was the lack of legal literature apparent but also a lack of public debate about these technologies. This lack of public debate and scrutiny and the paucity of legal analysis is matched by a virtual silence of national legislators and policy makers in this area. Theorists emphasise the critical need for transparency, accountability and public debate. The rational-critical communication theory, represented by Habermas and Jasanoff[5], has emerged in the social sciences and has helped to identify: a) the implicit theoretical assumptions for the deployment of biometric systems in immigration and criminal fields and b) the basis for the selection of an alternative theoretical foundation of assumptions of legal justifications for TBIF.

In regulation, privacy law, by default, has been the major regulatory framework for developments in TBIF. Yet little has been done to evaluate and analyse whether the specific context and development of ICT requires any modification or enhancement of the existing privacy regulatory framework internationally or domestically. This thesis addressed the challenge of balancing TBIF and a proper level of legal protection. Throughout of this thesis, the theme of the relationship between developments in biometrics and governments has been highlighted and the importance of citizens' need to know and debate about biometrics technology especially in regards to its deployment in immigration control and crime prevention contexts.

[4] See Chapter 2. Biometrics Systems: What is Biometrics?
[5] As elsewhere argued in this thesis the reasons advance to be openly and public debated or at least these reason publicly available. Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* (Princeton University Press, 2007) and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Einaudi, 1980).

8.3. Biometric industry: the Need for Self-Regulation

This thesis involved a mapping, albeit basic, of the rapidly developing biometric industry. A major factor in the limited, if not non-existent public debate about this industry has been the limited availability of public literature about the industry. Accordingly, it was necessary to undertake a mapping exercise to obtain an understanding of the industry. A website search methodology was developed and used to produce an illustrative map of the biometric industry. This preliminary website search identified a small number of key industry players, products and partnerships.

Although no surveys were conducted, the website methodology did reveal an industry with significant market concentration, key industry dominant companies and rapidly expanding uptake of these new biometric technologies. The concentrated biometric industry lacks, in the terms of Habermas and Jasanoff, “transparency, accountability and public debate”, whilst rapidly developing and generating millions of dollars of revenues. From the regulatory and legal standpoint, this expanding industry, whilst conscious of the national privacy practices at national levels had not developed any industry based guidelines or other regulatory standards towards establishing a self-regulated industry[6].

8.4. The emerging international regulatory framework

This industry and its widespread introduction of biometric systems and the consequent expansion of TBIF has proceeded with little national public awareness, discourse or formal regulation. The industry has not attempted to establish self-regulation standards. This industry is characterised by limited regulation or other intervention by national governments. At the national level, countries are relying exclusively on privacy and data protection laws to address the challenges and implications of TBIF in the two specific contexts of immigration information flow and

[6] See Chapter 3. The Biometric Industry: An Illustrative Map of Players, Products and Partnerships

information flow in criminal databases. Significantly, at the international level, there is no formal treaty regarding TBIF.

When biometric data, and for the purposes of this thesis, dealing with immigration information flow and information flow in criminal databases is exchanged across borders, rules developed and introduced by a range of official and semi-official international organisations apply. In the official category is the European Union (EU) and in the semi-official are organisations such as the international Civil Aviation Organisation (ICAO), the International Organization of Migration (IOM), the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC) and Interpol.

In the immigration context, this thesis identified two leading international organisations setting standards for the introduction of biometric systems: the International Civil Aviation Organisation (ICAO) and the International Organization of Migration (IOM). In addition, there are regional organisations moving towards biometric system standards as border control strategies, such as the European Union (EU) and the Asia Pacific Economic Cooperation (APEC). In addition, for cross-border personal data transfer there are two main international organisations making recommendations; in the semi-official category are the non-binding recommendations of the Organisation for Economic Co-operation (OECD) and, in the official category, the binding recommendations of the European Union[7].

In criminal context, there has been greater development of collaboration in relation to TBIF and, in particular there have been more formal bilateral or multilateral treaties regarding cross-border crimes. This collaboration has resulted in countries increasing the linkage between their national biometric criminal databases to international databases. Interpol has become a key player in relation to establishing rules in the context of TBIF. This has been the result of national concerns about terrorism, cross-border crimes and illegal immigration[8].

[7] See Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow
[8] See Chapter 5. Biometric Criminal Databases: Current Transborder Information Flow

8.5. TBIF in Immigration Information Flow and Information Flow in Criminal Databases

This thesis examined TBIF between immigration and criminal databases. The research involved using publicly available official reports and the limited published literature about TBIF in these contexts as well as conference presentations. The relevant legislation, principally on privacy and data protection was examined. The research included the organisation and conduct of semi-structured face-to-face interviews with academics and public officials in each of the four countries study jurisdictions[9]. The methodology developed and used in the semi-structured interviews was important. This research enabled the extent of the linkages of national databases and cross-border exchangeable biometric information in the immigration information flow and information flow in criminal databases contexts of the four jurisdictions to be fairly accurately established.

8.5.1. *Immigration Information Context*. In the immigration information flow context, this thesis demonstrated that the actual deployment of biometric systems is a measure to enhance border security and increase efficiency along the borders in the processing of travellers, stopping illegal immigrants, helping fight cross-border crimes and preventing terrorism. Importantly, the research identified asymmetries and convergences within TBIF representing legal challenges for governments. Legislators have generally failed to adequately address concerns about privacy and data protection and ensure that reform efforts in privacy or data protection laws have kept pace with TBIF developments[10].

The actual dynamics of TBIF in immigration information has been characterised by an absence of public debate[11] with attempts to combine not only national concerns but also international security interests. There are risks in centralised biometric

[9] This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011.
[10] See Chapter 4. Biometrics Systems in the Context of TransBorder Immigration Flow
[11] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 5 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 5.

databases for immigration purposes and their linkage with international biometric criminal databases.

The thesis noted the benefits of biometric systems and compared the actual ways in which the four countries collect immigration data. From the comparison, this thesis demonstrates the asymmetries on categories of data that are actually collected in relation to differences in the information collected and when that information is updated. The asymmetries revealed in the immigration context mirror those in the criminal records context. These asymmetries need to be, and can be addressed by the reinforcement of privacy or data protection laws[12].

8.5.2. *Information in Criminal Databases Context*. This thesis demonstrates the current operation of biometric criminal databases and the transition between the use of ordinary criminal databases and the implementation of biometric criminal databases at the national level. The thesis considers, at the international level, Interpol databases as an exemplar of best practices for an adequate uniform TBIF in crime prevention context through Interpol's standardisation in methods and systems[13].

This thesis identifies two modes of TBIF in the information flow in criminal databases context, namely the exchange of specific criminal information and the linkage of biometric criminal databases. The thesis also identifies the asymmetries among national biometric criminal databases posing significant barriers for a uniform TBIF[14] at the international level. The lack of transparency, accountability and public discussion[15] on processing and linking biometric databases is noted. The legal barriers to a harmonised TBIF are the asymmetries in collecting different criteria of biometric criminal information and targeting different people to be included. Therefore, these criminal record context asymmetries are similar to the legal

[12] For further details see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions
[13] For further details, see Chapter 5. Biometric Criminal Databases: Current Transborder Information Flow
[14] For further details, see Chapter 6. TransBorder Biometric Information Flows: Legal Challenges
[15] Jasanoff, Sheila, *Designs on Nature Science and Democracy in Europe and the United States,* above n 5 and Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", above n 5.

challenges is the immigration context. These concerns need to be and can be addressed by the reinforcement of privacy or data protection laws[16].

8.5.3. *Significant Common Legal Concerns: About TBIF*. This thesis discussed legal concerns in both immigration information flow and information flow in criminal databases contexts. In the four jurisdictions, the thesis demonstrates significant common legal concerns about TBIF in relation to immigration control and crime prevention context. The TBIF in both contexts is neither uniform nor consistent with respect of the information collected, stored, processed and exchanged. In addition, this thesis reveals some common legal challenges in privacy and date protection, which have studied since the inception of privacy regulation in the1980s and have yet to be resolved. These challenges are who can access data, data reliability (integrity), data protection in third party countries, the classification of individuals, data storage restrictions, and its impact on privacy[17]. This thesis, however demonstrates some new legal challenges because of the subsequent automated use of information[18]; the lack of binding recommendations; the lack of transparency, accountability and public debate regarding the operation and management not only in introducing biometric databases but also in the specific area of TBIF.

8.6. Recommendation to Address TBIF Legal Framework: A Privacy Approach

Recognising that the end of the journey to an emerging and common international framework has yet to be reached, this thesis proposes and recommends that national privacy and data protection regimes can provide realistic and achievable avenues to address the challenges of TBIF in the immigration and criminal databases contexts. The thesis identified two types of challenges in the area of privacy and data protection concerns; one is in relation to the actual automatic processing of the collection, storage and exchange of personal information and the other is actual use of the data and its inherent impact on an individual's privacy.

[16] For further details see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions
[17] For further details, see Chapter 6. Transborder Biometric Information Flows: Legal Challenges
[18] As it was discussed in section 6.3.6. Subsequent Automated Use of Information the new standard ANSI/NIST-ITL 1-2011 allows not only more amount of information, but also between dissimilar systems like immigration databases and criminal databases.

The thesis acknowledges that an international treaty for TBIF is highly unlikely. The main recommendation of this thesis; therefore is to reinforce legal protections in relation to TBIF, in the two specific contexts, by reinforcing existing privacy and data protection legislation at the national level. The effect of this recommendation will provide integrity and consistency in addressing challenges of TBIF in the two contexts and achieve consistency and common practices both nationally and internationally.

The thesis discussed three possible options of amendment of existing legislation; introducing specialised legislation; or, reinforcing administrative supervisory role of national Privacy Commissioners, a role which is already included in national privacy or data protection legislation. This thesis argued that the first two options are not politically achievable, do not guarantee effectiveness and may not be introduced in all jurisdictions. In addition, it is unlikely that the legislative processes of different countries could be coordinated to achieve uniform consistency in legislative amendments. The legislative process is complicated and takes time for final approval. The third option is more practical and achievable and requires only the agreement of Privacy Commissioners, which can be achieved administratively without legislation. This third option is to reinforce privacy authorities' supervisory powers in three main areas: the registration of biometric filing systems; cross-border co-operation agreements with other privacy or data protection agencies; and, promotion of individuals' rights for TBIF in a cross-border agenda[19].

The utilisation of the principle of proportionality, from its Civil Law tradition approach, is a synthetic method to determine justifiable interference with human rights in the public interest. By applying proportionality (reasonableness) test, transparency, accountability and public scrutiny, the thesis argued that reinforcing privacy and data protection frameworks, by empowering privacy authorities is a proportional response possible to resolve legal challenges of TBIF.

[19] For further details see Chapter 7. Transborder Biometric Privacy Regimes: National Solutions

8.7. Concluding Remark

TBIF is not a fashion that may disappear with time. On the contrary, it is an established practice that will continue. In fact, the amount of biometric information collected, stored, retrieved and exchanged will progressively increase. Therefore, TBIF must be seen as an increasingly important part of a sensitive legal privacy and data protection regime that requires a high level response in national legal frameworks. Legislators and policy makers must establish specific rules for governing TBIF. Revised legal frameworks should be publicly available and written in a way that all citizens can understand the implications not only of the deployment of biometric systems, but also, of their right to access their own information, the subsequent use of their biometric information, updates made to their personal information and, critically, about transborder exchanges. This thesis, hopefully is a contribution to the development of such national and international frameworks.

BIBLIOGRAPHY

CONSTITUTION AND INTERNATIONAL TREATIES

Constitution

Constitución Política de los Estados Unidos Mexicanos, DOF 05/02/1917 [Political Constitution of the United States of Mexico, last amended on 30/11/2012] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf (22/01/2013)

Bill of Rights Act 1990 (New Zealand)

Constitución Española, BOE num. 311 19/12/1978 [Spanish Constitution, last amended on 27/09/2011] (Spain) http://www.boe.es/buscar/act.php?id=BOE-A-1978-31229 (22/01/2013)

International treaties

American Convention on Human Rights, opened for signature 22 November 1969 (entered into force 18 July 1978)

American Declaration on the Rights and Duties of Man, adopted by the Ninth International Conference of American States, April 1948.

Convention on International Civil Aviation opened for signature 7 December 1944 (entered into force 4 April 1947)

International Declaration on Human Genetic Data, opened for signature and adopted 16 October 2003.

United Nations Convention against Transnational Organized Crime, opened for signature 15 November 2000 (entered into force 29 September 2003)

Universal Declaration of Human Rights, adopted by G/A/RES 217A (III) of 10 December 1948.

United Nations Global Counter-Terrorism Strategy, GA Res 60/288, UN GAOR, 116th sess, 117th plen mtg, Agenda Item 46, UN Doc A/Res60/288 (20 September 2006, adopted 8 September 2006)

Agreement on Operational and Strategic Cooperation between Australia and the European Police Office, signed 20 February 2007, ATS (entered into force according article 22)

INTERPOL MATERIAL

Constitution, General Assembly, 25th sess, adopted in June 1956 (came into force 13 June 1956)

Implementing rules on the processing of information for the purposes of international police co-operation (2009) http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts (21/12/2012)

Interpol (2009), *Interpol Handbook on DNA Data Exchange and Practice* http://www.interpol.int/INTERPOL-expertise/Forensics/DNA (21/12/2012)

*Rules governing access by an intergovernmental organization to the Interpol telecommunications network and databases http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts (*21/12/2012)

Rules on the Control of Information and access to INTERPOL's files (2010) http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts (21/12/2012)

Rules on the Processing of Information for the purposes of international police cooperation (RPI) (2008) http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts (21/12/2012)

Amended proposal for a Regulation of the European Parliament on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version), [2012] COM 2012/0254.

Charter of Fundamental Rights of the European Union [2010] OJ C 83/02.

Communication from the Commission to the Council and the European Parliament – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice, [2005] OJ C 236/24.

Communication from the Commission to the Council and the European Parliament - Towards enhancing access to information by law enforcement agencies (EU information policy), [2004] COD 2004/0429.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, on the Review of the EU regulatory framework for electronic communications networks and services, [2006] COD 2006/334.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1985), as amended by *The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, opened for signature 15 June 1995, (entered into force after acceptation by all Parties), as amended by the *Protocol to Convention ETS No. 108,* opened for signature 8 November 2001, ETS No. 181 (entered into force after acceptation by all Parties).

Convention implementing the Schengen Agreement, [1985] OJ L 239/22.

Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, [2008] OJ L 210/1.

Council of European Union, "SIS and SIRENE statistics-Guidelines to Collect Data" (2010) http://www.statewatch.org/news/2011/jan/eu-council-guidelines-data-sis-sirene-17436-10.pdf (22/12/2012)

Council Regulation (EC) No 2725/2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin, [2000] OJ L 316/15.

Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of

"Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, [2002] OJ L 62/1.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) of the European Parliament and of the Council, [2002] OJ L 201/37.

Directive 2009/136/EC (2009) amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, [2009] OJ L 337/11.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU),* 5 September 2012.

Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, [2009] OJ C 88/6.

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2012] COD 2012/0011.

Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted 23 November 2010.

Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies, adopted 9 September 1991.

Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals, [2003] OJ L 157/15.

Regulation (EC) 1683/95 laying down a uniform format for visa, [2003] OJ L164/14.

Regulation (EC) 333/2002 on a uniform format for forms for affixing the visa issued by Member States to persons holding travel documents which are not recognised by the Member State drawing up the form, [2002] OJ L 53/23.

Regulation (EC) No 444/2009 of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, [2009] OJ L 142/6.

Resolution (74)29 related to the protection of individuals vis-à-vis electronic data banks, adopted 20 September 1974.

LEGISLATION

Australia

Civil Aviation Legislation (Mutual Recognition with New Zealand) Act 2006 (Cth)

Crimes Act 1914 (Cth)

Criminal Code Act 1995 (Cth)

Migration Act 1958 (Cth)

Privacy Act 1988 (Cth)

Mexico

Código Penal Federal, DOF 14/08/1931 [Federal Criminal Code, last amended on 14/06/2012] http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf (21/12/2012)

Ley de Aviación Civil, DOF 12/05/1996 [Federal Civil Aviation Law last amended on 21/05/2013] http://www.diputados.gob.mx/LeyesBiblio/pdf/25.pdf (21/12/2012)

Ley de la Policía Federal, DOF 25/05/2011 [Federal Police Law] http://www.diputados.gob.mx/LeyesBiblio/pdf/LPF.pdf (21/12/2012)

Ley de Migración, DOF 25/052011 [Migration Law] http://www.diputados.gob.mx/LeyesBiblio/pdf/LMigra.pdf (20/12/2012)

Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares, DOF 5/07/2010 [Federal Data Protection in Possession by the Private Sector Act] *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf* (21/12/2012)

Ley Federal de Transparencia y Acceso a la Información Pública, DOF 11/06/2002 [Federal Transparency and Access to Governmental Public Information last amended on 08/06/12] http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf (21/12/2012)

Ley General de Población, DOF 07/01/1974 [General Population Law, last amended on 09/04/12] http://www.diputados.gob.mx/LeyesBiblio/pdf/140.pdf (20/12/2012)

Ley General del Sistema Nacional de Seguridad Pública, DOF 02/01/2009 [General Law of National System of Public Security, last amended on

28/12/2012] http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf (21/12/2012)

Ley sobre Refugiados y Protección Complementaria, DOF 27/01/2011 [Refugees and Complementary Protection Law] http://www.diputados.gob.mx/*LeyesBiblio*/pdf/LRPC.pdf (20/12/2012)

New Zealand

Civil Aviation Act 1990 (New Zealand)

Criminal Investigations (Bodily Samples) Amendment Act 2003 (New Zealand)

Criminal Investigations (Bodily Samples) Amendment Act 2009 (09/46) (New Zealand)

Criminal Investigations (Bodily Samples) Act 1995 No. 55 (as at 01 October 2010)

Electronic Identity Verification Act 2012 (New Zealand)

Human Rights Act 1993 (New Zealand)

Identity Information Confirmation Act 2012 (New Zealand)

Immigration Act 2009 (New Zealand)

Privacy Act 1993 (New Zealand)

Spain

Ley 21/2003, de 7 de Julio, de Seguridad Aérea, BOE-A-2003-13616 [Law 21/2003 of 7 July, security aviation, last amended 1 March 2014] http://www.boe.es/buscar/pdf/2003/BOE-A-2003-13616-consolidado.pdf (21/12/2012)

Ley 59/2003, de 19 de diciembre, de firma electrónica, BOE-A-2003-23399 [Law 59/2003 of 19 December, electronic signature] http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399 (19/12/2012)

Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, BOE-A-1992-4252 [Organic Law 1/1992 of 21 February, on the Protection of Public Safety] http://www.boe.es/buscar/doc.php?id=BOE-A-1992-4252 (19/12/2012)

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, BOE-A-1995-25444 [Organic Law 10/1995 Criminal Code] https://www.boe.es/buscar/doc.php?id=BOE-A-1995-25444 (21/12/2012)

Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, BOE-A-2007-17634 [Organic Law 10/2007 regulating the police database on identifiers obtained from DNA] http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-17634 (21/12/2012)

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE-A-1999-23750 [Organic Law 15/1999 of 13 December, on the Protection of Personal Data] http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 (21/12/2012)

Ley Orgánica 2/2009, de 11 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, BOE-A-2009-19949 [Organic Law 2/2009 amending the Organic Law 4/200 regarding Rights and Liberties for Foreigners in Spain and their Social Integration] http://www.boe.es/buscar/doc.php?id=BOE-A-2009-19949 (20/12/2012)

Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, BOE-A-2000-544 [*Organic Law 4/2000 about Rights and Liberties for Foreigners in Spain and their Social Integration] http://www.boe.es/buscar/act.php?id=BOE-A-2000-544* (20/12/2012)

Real Decreto 1161/2009, de 10 de julio, por el que se modifica el Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España de ciudadanos de los Estados miembros de la Unión Europea y de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo, BOE-A-2007-4184, [Royal Decree on the entry, free movement and residence in Spain of citizens of the Member States of the European Union and other States party to the Agreement on the European Economic Area] http://www.boe.es/buscar/doc.php?id=BOE-A-2007-4184 (20/12/2012)

Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, BOE-A-2005-21163 [Royal Decree 1553/2005 of 23 December, regulating the issue of national identity and electronic signature certificates] http://www.boe.es/buscar/doc.php?id=BOE-A-2005-21163 (19/12/2012)

CASES

Australia

South Australia v Tanner (1989) 166 CLR 161

Australian Broadcasting Tribunal v Bond (1990) 170 CLR 321

Canada

D v Barraeu du Quebec, [2012] SCC 12

R v Oakes, [1986] 1 SCR 103

Spain

Sentencia Tribunal Constitucional [Constitutional Tribunal Sentence], 66/1995, 8 May 1995, 13 June 1995 published in BOE. http://www.boe.es/buscar/doc.php?coleccion=tc&id=SENTENCIA-1995-0066

Recurso de Inconstitucional [Constitutional Complaint] 292/2000, 20 November 2000, 4 January 2001 published in BOE. http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf (23/12/2012)

Inter-American Court of Human Rights

Advisory Opinion OC-6/86 (1986) 6 Inter-American Court HR (ser A)

Gonzalez et. al. ("Cotton Field") v. Mexico (2009) 113 Inter-American Court HR (ser C)

Kimel v. Argentina (2008) 177 Inter-American Court HR (ser C)

European Court of Human Rights

Amann v. Switzelard (European Court of Human Rights, Grand Chamber, Application No 27798/95, 16 February 2000)

Klass and Other v. Germany, (1978) 214 Eur Court HR (ser A)

Leander v. Sweden (1987) 116 Eur Court (ser A)

Marper v. The United Kingdom (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008)

P.G. and J.H. v. The United Kingdom (European Court of Human Rights, Application No 44787/98, 25 September 2001)

Peck v the United Kingdom (2003) 36 EHRR 41, EMLR 287

Sciacca v. Italy (European Court of Human Rights, Application No 50774/99, 11 January 2005)

Valenzuela v. Spain (1998) Eur Court HR

Young, James and Webster v *United Kingdom* (European Court of Human Rights, Plenary, Application Nos 7601/76 and 7806/77, 13 August 1981) 63.

X and Y v. The Netherlands (1985) 91 Eur Court (ser A)

OFFICIAL AND UNOFFICIAL REPORTS

Australia Governments, Australian Customs and Border Protection Service, *The Blueprint for Reform* (2013-2018) http://www.customs.gov.au/site/Reformquicklinks.asp (21/07/2013)

Australia Government, Australian National Audit Office, *Audit Report* No 24 (*2007-2008)* *http://www.anao.gov.au/~/media/Uploads/Documents/2007%2008_audit_report_24.pdf* (20/12/2012)

Australia Government, Australian Privacy Commissioner, *Explanatory Statement*, *The Privacy Act 1988* (Cth) 1-5. http://www.comlaw.gov.au/Details/F2012L00869/Explanatory%20Statement/Text (19/12/2012)

Australia Government, CrimTrac*, Full Report (Annual Report for 2009-10)* http://www.crimtrac.gov.au/documents/CrimTrac_0910_full.pdf (21/12/2012)

Australia Government, Department of Immigration and Citizenship, *Annual Report* (2008-2009), http://www.immi.gov.au/about/reports/annual/2008-09/pdf/annual-report-2008-09-complete.pdf (20/12/2012)

Australia Government, Department of Immigration and Citizenship, *Review of Personal Identifier Provisions Introduced In 2004 to Migration Act 1958,* Final Report (2009) http://www.immi.gov.au/media/publications/pip-review/pip-review.pdf (20/12/2012)

Australia Government, Department of Immigration and Citizenship, *Annual Report (2010-2011)* http://www.immi.gov.au/about/reports/annual/2010-11/html/outcome-3/identity.htm (20/12/2012)

Australia Government, Department of Immigration and Citizenship, *Annual Report* (2011-2012), http://www.immi.gov.au/about/reports/annual/2011-12/html/ (20/12/2012)

Australia Government, Department of Immigration and Citizenship, *The People of Australia- Australia's Multicultural Policy*, (2011) http://www.immi.gov.au/about/reports/annual/2008-09/pdf/annual-report-2008-09-complete.pdf (20/12/2012)

Australia Government, Office of Regulation Review 1998, *A Guide to Regulation (second edition)* *http://www.pc.gov.au/__data/assets/pdf_file/0006/66876/reguide2.pdf* (21/07/2013)

European Union Committee, House of Lords, *Schengen Information System II (SIS II),* 9th Report of Session 2006-07 (2007)

ICAO, "The Implementation of ePassports", *MRTD Report No. 3* (2012) http://www.icao.int/publications/journalsreports/2012/MRTD_Report_Vol7_No3.pdf (19/12/2012)

ICAO, *Selection of a Globally Interoperable Biometric for Machine Assisted Identity Confirmation with MRTDs*, Technical Report (2001) http://www.icao.int/Security/mrtd/Downloads/Technical%20Reports/ICAO_MRTD_History_of_Interoperability.pdf (27/11/2012)

ICAO, "Why ICAO selected the face as primary biometric identifier specified to epassports", *MRTD Report* (2007) http://www2.icao.int/en/MRTD2/ReportsPastIssues/ICAO%20MRTD%20Report%20Vol.%202%20No.%201,%202007.pdf (20/12/2012)

IOM, *Migration initiatives 2012* (2012) http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/published_docs/books/Migration-Initiatives-Appeal.pdf#australia (20/12/2012)

IOM, *Migration Initiatives Appeal 2010* (2010) http://publications.iom.int/bookstore/free/Migration_Initiatives_2010.pdf (20/12/2012)

Mexico Government, Inter-American Development Bank, *Strategic Planning Project "Platform Mexico,* Technical cooperation profile (2008) http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=1397559 (21/12/2012)

Mexico Government, Minister of Public Security, *Platform Mexico,* 1st Report of Duty 2006-2007 (2007) http://pdba.georgetown.edu/Security/citizensecurity/Mexico/evaluaciones/InformeLabores-plataformamexico.pdf (21/12/2012)

Mexico Government, National Commission for the Protection and Defense of Users of Financial Services, *Fines imposed on financial institutions,* (2012) http://www.condusef.gob.mx/PDF-s/Comunicados/2012/com05_multas-2011.pdf (19/12/2012)

Mexico Government, National Institute of Migration*, Action Lines in Sector Programs Accountability, Transparency and Fighting Corruption committed in 2009* Final Report (2008-2012) http://www.inm.gob.mx/static/transparencia/PND/Formatos_A_y_B.pdf (20/12/2012)

Mexico Government, Presidential Office, *First Report regarding the Application of the National Development Plan 2007-2012*, Rule of Law and Security (2007) http://pnd.presidencia.gob.mx/pdf/PrimerInformeEjecucion/1_3.pdf (21/12/2012)

New Zealand Government, *Immigration Act Review* (April 2006) http://www.dol.govt.nz/PDFs/immigration-act-review-overview.pdf (20/12/2012)

New Zealand Government, Inland Revenue*, Annual Report* (2012) http://www.ird.govt.nz/resources/1/4/14a3ef004d1a9cf8915793d981e6622f/annual-report-2012.pdf (19/12/2012)

New Zealand Government, States Services Commission, *Communication Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management* (2009) http://ict.govt.nz/library/offshore-ICT-service-providers-april-2007.pdf (23/12/2012)

OECD, *Recent changes in Migration Movements and Policies: country notes* (2010)

OECD, *Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy,* Report 178 (2011)

OECD, *Report on the Cross-Border Enforcement of Privacy Law,* Report 121 (2006) http://dx.doi.org/10.1787/231304814207 (23/12/2012)

OECD, *Biometric-based Technologies*, Report 101 (2004) http://dx.doi.org/10.1787/232075642747 (22/08/2012)

United States Government, United States Department of Commerce, National Telecommunications and Information Administration, *Privacy and Self-regulation in the information age*, (1997) http://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age (19/12/2012)

PARLIAMENTARY DEBATES AND SUBMISSION TO GOVERNMENTS

Parliamentary debates

(7 February 2012) 677 NZPD 138

Submission to Government inquiries, committees and agencies

Australia Government “Consideration to the Asia Pacific Economic Cooperation (APEC) on the Proposed Business Mobility Goals for 2009”

European Data Protection Supervisor “Opinion to the European Parliament on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…]”.https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/2012-09-05_edps_opinion_on_eurodac.pdf (24/12/2012)

New Zealand Privacy Commissioner “Submission to the Government Administration Committee on the Electronic Identity Verification Bill”.

UNHCR “Comments to the European Parliament on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…]” http://www.unhcr.org/50adf9749.pdf (24/12/2012)

GUIDELINES/ETHIC CODES/MANUALS

International

APEC Cross-Border Privacy Rules System (2012) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx (27/09/2012)

APEC *Guiding Principles for PKI-Based Approaches to Electronic Authentication* (2005) http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel/annex_d.aspx (20/12/2012)

APEC Privacy Framework (2004) http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (23/12/2012)

ICAO Machine Readable Travel Documents, DOC 9303 http://www.icao.int/publications/pages/publication.aspx?docnum=9303 (19/12/2012)

ICAO Machine Readable Travel Documents Supplement to DOC 9303 http://www.icao.int/Security/mrtd/Documents/Supplement%20to%20ICAO%20Doc%209303%20-%20Release_13.pd (31/03/2014)

Joint Supervisory Authority of Schengen, *The Schengen Information System. A guide for exercising the right of access* (2009) http://www.dutchdpa.nl/downloads_int/Guide_for_exercising_the_right_of_access.pdf (22/12/2012)

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD Council, 1037th sess (25 July 2002) http://www.oecd.org/internet/interneteconomy/15582260.pdf (23/12/2012)

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD (23 September 1980) http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (18/12/2012)

OECD Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007) http://www.oecd.org/internet/interneteconomy/38770483.pdf (23/12/2012)

OECD Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (2011) http://dx.doi.org/10.1787/5kg2b7l7pljk-en (23/12/2012)

UN Recommendations on Statistics of International Migration, UN Department of Economic and Social Affairs Statistics Division (1998) http://unstats.un.org/unsd/publication/SeriesM/SeriesM_58rev1E.pdf (20/12/2012)

Australia

Department of Immigration and Citizenship, *Australia's PP Advanced Passenger Processing System Check-in Guide,* (October 2008) http://www.immi.gov.au/media/publications/visa-entry/_pdf/APP_Guide_full_manual.pdf (22/12/2012)

Office of the Privacy Commissioner of Australia, *Guidelines to the National Privacy Principles* (2001) http://www.privacy.gov.au/materials/types/guidelines/view/6582 (23/12/2012)

Office of the Privacy Commissioner of Australia, *Private sector information sheet 30 – ID scanning in pubs and clubs*, (April 2010) http://www.privacy.gov.au/materials/types/infosheets/view/7074 (19/12/2012)

Photo guidelines https://www.passports.gov.au/images/photo_guidelines.pdf#zoom=100 (20/12/2012)

Mexico

Acuerdo por el que se dan a conocer el Manual de Captura de Información y el Manual de Intercambio de Información, DOF 21/09/2006 [Manual of Collection and Exchange of Information] http://www.normateca.gob.mx/Archivos/32_D_1092_07-11-2006.pdf (21/12/2012)

Acuerdo por el que se expide el Manual de Criterios y Tramites Migratorios del Instituto Nacional de Migración, DOF 29/01/2010, [Manual of Criteria and Migratory Proceedings of the National Institute of Migration of the Minister of Interior of 21 September 2010] (Mexico) http://dof.gob.mx/nota_detalle.php?codigo=5129775&fecha=29/01/2010 (20/12/2012)

Conectividad a la Plataforma México [Connectivity Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-cpm-10_1.pdf (21/12/2012)

Integración, Consulta y Actualización del Registro de Huellas Dactilares [Integration, Consultation and Record Updating Fingerprint] (April 2010)

http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-rehd-10_1.pdf (21/12/2012)

Photo guidelines http://www.sre.gob.mx/index.php/primera-vez/252 (20/12/2012)

Seguridad Lógica de la Plataforma México [Logical Security Platform Mexico] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-slpm-10_1.pdf (21/12/2012)

Sistema de Identificación de Personas Mediante Análisis de Voz [People Identification System Using Voice Analysis] (April 2010) http://portal.secretariadoejecutivosnsp.gob.mx/webfiles/pdf/cni-sav-10_1.pdf (21/12/2012)

New Zealand

Photo guidelines http://www.passports.govt.nz/Passport-photos---adults (20/12/2012)

Spain

Dirección General de la Policía y Guardia Civil, *DNI Electrónico Guía de Referencia Básica*, Comisión Técnica de Apoyo a la Implementación del DNI Electrónico (2010) [Basic Electronic Guide eID] (Spain) http://www.dnielectronico.es/Guia_Basica/index.html (19/12/2012)

Photo guidelines http://www.interior.gob.es/pasaporte-29/clases-y-requisitos-183?locale=es (20/12/2012)

BOOKS

"Bertillon system". *Encyclopædia Britannica. Encyclopædia Britannica Online.* Encyclopædia (Britannica Inc., 2013) http://www.britannica.com/EBchecked/topic/62832/Bertillon-system (9/12/2012)

Alexander, Larry (ed), *Constitutionalism Philosophical Foundations* (Cambridge University Press, 1998).

Andrews, Lori B., *Future Perfect, Confronting Decisions about Genetics*, (Colombia University Press, 2001).

Águila, Rafael del *Manual de Ciencia Política* (Editorial Trotta, 5th ed, 2008).

Aragón, Manuel, *Constitución, Democracia y Control*, (Instituto de Investigaciones Jurídicas de la UNAM, 2002).

Aries, Phillippe and Duby, Georges, *Historia de la Vida Privada*, (Taurus, 1989) vol. 5.

Ashbourn, Julian, *Biometrics: advanced identity verification. The complete guide*, (Springer, 2000).

Ashenden, Samantha and Owe, David, *Foucault Contra Habermas,* (Sage Publications, 1999).

Battle Sales, Georgina, *El Derecho a la Intimidad Privada y su Regulación,* (Marfil, 1972).

Beavan, C., *Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science,* (Hyperion, 2001).

Beyleveld, Deryck and Brownsword, Roger, *Human Dignity in Bioethics and Biolaw*, (Oxford University Press, 2004).

Bidgoli, Hossein (ed), *Global Perspectives in Information Security, Legal, Social and International Issues*, (John Wiley & Sons Inc., 2009).

Bogdandy Armi von, Ferrer Mac-Gregor, Eduardo and Morales Antoniazzi, Mariela (coords), *La Justicia Constitucional y su Internacionalizacion. Hacia un Ius Constitucionale Commune en America Latina?,* (UNAM, Instituto Iberoamericano de Derecho Constitucional, Max-Planck-Institut Für Ausländisches Öffentliches Recht Und Völkerrecht, 2010).

Bolle, Ruud M., *et. al., Guide to Biometrics*, (Springer, 2003).

Boucher, David and Kelly, Paul, *The Social Contract From Hobbes to Rwals*, (Routledge, 1994).

Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010).

Bovenberg, Jasper A., *Property Rights in Blood, Genes and Data, Naturally Yours?* (Martinus Nijhoff Publishers, 2006).

Braithwaite, John, "Responsive Regulation in Australia" in Grabosky, Peter y Braithwaite John (eds.), *Regulation and Australia's Future*, (Australian Institute of Criminology, 1993).

Bresler, Jack, B. (ed), *Genetics and Society*, (Addison-Wesley Publishing Company, 1973).

Bridwell, Randall and Whitten, Ralph U., *The Constitution and the Common Law*, (Lexington Books, 1997).

Carvan, John, *Understanding the Australian Legal System*, (Thomson Reuters, 6th ed, 2010).

Chalmers D., *Genetic Testing in the Criminal Law*, (UCL Press, 2007)

Chen, H. et. al., *National Security. Handbook in Information Systems*, (ELSEVIER, 2007) vol. 2.

Cholewinski, Ryszard, *et. al., International Migration Law: Developing Paradigms and Key Challenges,* (T.M.C. Asser Press and International Organization for Migration, 2007).

Crock Mary and Berg Laurie, *Immigration Refugees and Forced Migration, Law, Policy and Practice in Australia,* (The Federation Press, 2011).

Collins, Alan, *Contemporary Security Studies,* (Oxford University Press, 2007).

Darwin, Charles, *On the Origin of Species,* (Murray, 1859).

Day, David, "Biometric Applications, Overview", *Encyclopaedia of Biometrics,* (Springer, 2009). http://springerlink.metapress.com/content/q22t17844168/fulltext.pdf (18/12/2012)

Douzinas, Costas, *The End of Human Rights Critical Legal Thought at the Turn of the Century*, (Hart Publishing, 2000).

Edgar, Andrew, *The Philosophy of Habermas*, (Acumen Publishing Limited, 2005).

Eriksen, Erik Oddvar and Weigard, Jarle, *Underastanding Habermas, Communicative Action and Deliberative Democracy*, (Continuum, 2003).

Ernst, Morris L. And Schwartz Alan U., *The Right to be Let Alone*, (MacMillan Co, 1962).

Fariñas Matoni, Luis María, *El Derecho a la Intimidad*, (Trivium, 1983).

Farrar H, John, *Legal Reasoning*, (Thomson Reuters, 2010).

Fioravanti, Mauricio, *Los Derechos Fundamentales: Apuntes de Historia de las Constituciones,* (Trotta, 2003).

Fischer, F. Citizens, experts, and the environment: The politics of local knowledge, (Duke University Press, 2000)

Galton, Francis, *Natural inheritance* (MacMillan, 1889)

García De Enterría, Eduardo, *La Constitución como norma y el Tribunal Constitucional*, (Editorial Civitas, 2006).

Gerth, H. H. And Wright Mills, L. (ed.) *From Max Webber, Essays in Sociology*, (Rutledge, 2009).

Goldie, Mark, *John Locke, A Letter Concerning Toleration and Other Writings* (Liberty Fund, 2010) http://files.libertyfund.org/files/2375/Locke_1560_EBk_v6.0.pdf (18/12/2012)

Gozaíni, Osvaldo Alfredo, *Derecho Procesal Constitucional, Hábeas Data, Protección de datos personales*, (Rubinzal-Culzoni Editores, 2001).

Habermas, Jürgen, "Sfera pubblica (Una voce di enciclopedia)", *Cultura e Critica*, (Einaudi, 1980).

Habermas, Jürgen, *The Theory of Communicative Action* (Thomas McCarthy trans, Beacon Press, 1984)

Habermas, Jürgen, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society (Studies in Contemporary German Social Thought)*, (Massachusetts Institute of Technology, 1991).

Habermas, Jürgen, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (William Rehg trans, MIT Press, 1996).

Habermas, Jürgen, *The Inclusion of the Other: Studies in Political Theory*, (Ciaran Cronin and Pablo De Greiff trans, MIT Press 1998).

Hall, Kath and Macken, Claire, *Legislation and Statutory Interpretation*, (Lexis Nexis Butterworths, 2nd ed, 2009).

Hartwell, Leland *et.al.*, *Genetics from Genes to Genomes*, 3rd ed, (McGraw Hill, 3rd ed, 2008).

Havelock, Ellis, *The Criminal*, (Scribner & Welford, 1890). http://archive.org/details/criminal00elli (09/12/2012)

Heath Wellman, Christopher and Cole, Phillip, *Debating the Ethics of Immigration, Is there a Right to Exclude?* (Oxford University Press, 2011)

Hiler, Sean P. And Greenberg, *The Surveillance Studies Reader*, (McGraw Hill, Open University Press, 2007).

Jackson, Margaret, *Hughes on Data Protection in Australia*, (LawBook Co, 2001).

Jackson, Margaret, and Shelly, Marita, *Electronic Information and the Law*, (Thomson Reuters, 2012).

Jain, Anil K., Flynn, Patrick and Ross, Arun A., *Handbook of Biometrics*, (Springer, 2008).

James, B. Rule and Greenleaf, Graham, *Global Privacy Protection. The First Generation*, (Elgar Publishing Inc., 2008).

Jasanoff, Sheila, *Designs on Nature, Science and Democracy in Europe and the United States,* (Princeton University Press, 2007).

Kabera, Stephen, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation,* (Nartinus Nijhoff Publishers, 2008).

Kevles, Daniel J. And Hood, Leroy (eds), *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, (Harvard University Press, 1993).

King, Robert C. And William D., Stansfield, *A Dictionary of Genetics*, (Oxford University Press, 5th ed, 1997)

Krane, Dan, *et. al., Fundamental Concepts of Biometrics*, (International Edition, 2003).

Kuschewsky, Monika (ed.), *Data Protection and Privacy Jurisdictional Comparison,* (Thomson Reuters, 2012)

Locard, Edmond, *Manual de Técnica Policiaca*, (Editorial Maxtor, 1935).

Lyon, David, *Surveillance Society Monitoring Every Day Life,* (Open University Press, 2001).

Lyon, David, *Surveillance Studies an Overview*, (Polity Press, 2007).

Lyon, David, *Identifying Citizens: ID Cards as Surveillance* (Polity, 2009)

Lyon, David, and Bennett, Colin (eds.) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (Routledge, 2008)

Márquez Romero, Raúl (ed.) *Lineamientos y Criterios del Proceso Editorial*, (Universidad Nacional Autonoma de Mexico, 2008) http://www.juridicas.unam.mx/publica/critedit/critedit.pdf (22/01/2013)

Marx, G.T., "Technology and Social Control", *International Encyclopaedia of the Social & Behavioural Sciences*, (Elsevier, 2001).

Mather, Kenneth and Jinks, John L., *Biometrical Genetics. The study of continuous variation*, (Cornell University Press, 1971).

McArdle, J.J. and Allison, D.B., "Genetic Studies of Behaviour: Methodology", *International Encyclopaedia of the Social & Behavioural Sciences*, (Elsevier, 2001).

McPherson, C.B., *John Locke Second Treatise of Civil Government* (Hackett Publishing Company, 1980) http://oregonstate.edu/instruct/phl302/texts/locke/locke2/locke2nd-a.html (18/12/2012)

Merryman, John Henry and Perez-Perdomo, *The Civil Law Tradition. An Introduction to the Legal systems of Europe and Latin America,* (Stanford University Press, 3rd ed, 2007).

Moore, Bruce (ed), *Australian Concise Oxford Dictionary*, (Oxford University Press, 5th ed, 2009).

Morales Prats, Fermín, *La tutela penal de la intimidad: privacy e informática*, (Destino, 1984).

Mulholland, R.D., *Introduction to the New Zealand Legal system*, (Butter Worths, 1976).

Nicholas, Emiliou, *The principle of proportionality in European law: A comparative study,* (Kluwer Law International, 1996).

Nieto, Santiago, *et. al.*, *Control externo y responsabilidad de los servidores públicos del Distrito Federal,* (Universidad Nacional Autonoma de Mexico, 2005).

Nino, Carlos, *La constitución de la democracia deliberativa*, (Gedisa, 1997).

Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical issues*, (Cambridge Publishers, 2007).

Payne, Rodger A. and Smahat, Nayef H., *Democratizing Global Politics, Discourse Norms, International Regimes and Political Community*, (State University of New York Press, 2004).

Pérez Luño, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución,* (Tecnos, 2003).

Pérez San-José, Pablo (Dir.), *Estudio sobre las tecnologías biométricas aplicadas a la seguridad,* (Instituto Nacional de Tecnologías de la Comunicación, 2011)

Penk, Stephen *et. al.*, *Privacy Law in New Zealand*, (Thomson Reuters, 2010)

Rabibnow, Paul and Nikolas, Rose (eds.) The Essential Foucalt 1954-1984, (The New Press, 2003)

Rebollo Delgado, Lucrecia, *El Derecho Fundamental a la Intimidad,* (Dykinson, 2005).

Reeve, Eric C.R. (ed). "Statistics", *Encyclopaedia of Genetics*, (Fitzroy Dearborn Publishers, 2001).

Richard Perruchoud (ed), "Glossary on Migration", *International Migration Law*, (IOM, 2004) http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/published_docs/serial_publications/Glossary_eng.pdf (20/12/2012)

Romeo Casabona, Carlos Maria (ed), *Bases de datos de perfiles de ADN y criminalidad*, (Cátedra Interuniversitaria, Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, 2002).

Romeo Casabona, Carlos and Sergio, Romeo Malanda, *Los Identificadores del ADN en el Sistema de Justicia Penal*, (Aranzadi, 2010).

Ruiz Miguel, Carlos, *La Configuración Constitucional del Derecho a la Intimidad,* (Tecno, 1995).

Rule, James B and Greenleaf, Graham, *Global Privacy Protection*, (Edward Elgar Publishing, 2008).

San Agustín Confesiones (Eugène Portalié trans, Prana, 2006)

Sanchez Gil, Ruben, *El principio de proporcionalidad*, (Universidad Nacional Autonoma de Mexico, 2007).

Sartori, Giovanni, *Homo Videns, la sociedad teledirigida,* (Taurus, 2004).

Saunders Cheryl, *It's Your Constitution Governing Australia Today*, (The Federation Press, 2003).

Saunders Cheryl, *The Constitution of Australia*, *A contextual Analysis,* (Hart Publishing, 2011).

Shoniregun, Charles A. and Crosier, Stephen, *Securing Biometrics Applications,* (Springer, 2008).

Sloan Coats, William (ed), *The Practitioner's Guide to Biometrics*, (ABA Publishing, 2007).

Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, (W.H. Freeman and Company, 1973).

Sokal, Robert and James, Rohlf, *Biometry*, (W.H. Freeman and Company, 3rd ed, 2003).

Stallings, William, *Data and Computer Communications*, (Prentice Hall, Upper Saddle River, 2004).

Tamayo y Tamayo, Mario, *El Proceso de la Investigación Científica*, (LIMUSA, 2011)

Turak, Daniel C., *The Passport in International Law*, (Lexington Books, 1972).

Ugalde, Luis Carlos, *La rendición de cuentas en los gobiernos estatales y municipales,* (Auditoría Superior de la Federación, 2002).

Van Krieken, Peter J. (ed), *Terrorism and the International Legal Order, With special Reference to the UN, the EU and Cross-Border Aspects*, (T.M.C. Asser Press, 2002).

Villanueva, Ernesto, *Derecho de la información*, (Porrúa-Cámara de Diputados-Universidad de Guadalajara, 2006).

Watson, Alan, *Comparative Law: Law, Reality and Society*, (Vandeplas Publishing, 3rd ed, 2010).

Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005).

Webb, Duncan, *et. al.*, *The New Zealand Legal System*, (Lexis Nexis, 2010).

Weber, Leanne and Pickering Sharon, *Globalization and Borders. Death at the Global Frontier,* (Palgrave MacMillan, 2011).

Williams, Paul D. *Security Studies. An Introduction,* (Routledge, 2008).

Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003).

Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000).

ARTICLE JOURNALS

Ackerman, John and Sandoval Ballesteros, Irma, “The global explosion of freedom of information laws” (2006) 58 *Administrative Law Review* 85-130.

Anderson, keith “Is There Still a Sound Legal Basis: The Freedom of Information Act in the Post 9/11 World” (2003) 69 *Ohio St. Law Journal* 342-368

Armitage, Peter, “Biometry and Medical Statistics” (1985) 41 *Biometrics* 823-833.

Barkawi, Tarak and Laffey, Mark (eds.) “The post-colonial moment in security studies” (2001) 32(2) *Review of International Studies* 329-352

Black, Julia, “Constitutionalising Self-Regulation”, (1996) 59(1) *The Modern Law Review* 24-55

Black, Julia, “Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a “Post-Regulatory” World”, (2001) 54(1) *Current Legal Problems* 103-146

Boudin, Leonard B., “The Constitutional Right to Travel” (1956) 56 *Columbia Law Review* 47-75.

Bygrave, Lee, “Privacy Protection in a Global Context -A Comparative Overview”, (2004) 47 *Scandinavian Studies in Law* 319-348.

Bygrave, Lee, “The Place of Privacy in Data Protection Law” (2001) 24(1) *University of New South Wales Law Journal* http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (18/12/2012)

Cooper, David M., “Transborder data flow and the protection of privacy: the harmonization of data protection law” (1984) 8 *Fletcher Forum* 339-352.

Cowen, Zelman "The Private Man" (1969) *The Boyer Lectures*, Australian Broadcasting Commission 9-10.

Davies, S., “The Brave new world of biometric identification” (1995) 2 *Privacy Law and Policy Reporter* 30.

Diaz, Vanessa, “Sistemas Biometricos en material criminal: un estudio comparado [Biometric Criminal Databases: a comparative study]” (2013) 31(7) IUS *Revista del Instituto de Ciencias Juridicas de Puebla* 28-47.

Dieter, Grimm “Proportionality in Canadian and German Constitutional Jurisprudence” (2007) 57 (2) *University of Toronto Law Journal* 383-397.

Doyle, C., “Self-Regulation and Statutory Regulation” (1997) 8(3) *Business Strategy Review* 35-42.

Epstein, Charlotte, “Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders” (2007) 1 *International Political Sociology* 149-164.

Farral, Lyndsay A., “Controversy and Conflict in Science: a Case Study –The English Biometric School and Mendel’s Laws” (1975) 5 *Social Studies of Science* 269-301.

Galton David J. and Galton Clare J. “Francis Galton and Eugenics Today” (1998) 24(2) *Journal of Medical Ethics* 99-105.

Gavison, Ruth “Privacy and the Limits of Law” (1980) 89(3) *The Yale Law Journal Company* 421-471.

Hopkins, Richard, “An introduction to biometrics and large scale civilian identification*”* (1999) 13(3) *International Review of Law, Computers & Technology* 337-363.

Herschel, William J. “The Origin of Finger-Printing” 2004 *Oxford University Press*, Digital edition by Gavan Tredoux in http://galton.org/fingerprints/books/herschel/herschel-1916-origins-1up.pdf (18/12/2012)

Kirby, Michael, “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy” (2010) 20(2) *Journal of Law, Information and Science* 1-14.

Martínez Pisón, José, “Vida Privada: Implicaciones y Perversiones”, (1997) XIV *Anuario de Filosofía del Derecho* 720-723.

Michaelsen, Christopher, “The Proportionality Principle, Counter-terrorism Laws and Human Rights: A German-Australian Comparison”, (2010) *Berkeley Electronic Press,* 2:1. http://law.bepress.com/cgi/viewcontent.cgi?article=1230&context=unswwps-flrps10 (23/12/2012)

Mueller, Gerhard O. W. “Transnational Crime: Definitions and Concepts,” (1998) 4 *Transnational Organized Crime* 13-21.

Nava Gomar, Salvador Olimpo*, “*El Estado constitucional: sinonimia positivizada entre Constitución y democracia (triple relación)” (2003) *Anuario de Derecho Constitucional Latinoamericano* 14-34.

Norton, B.J., “The Biometric Defense of Darwinism” (1973) 6(2) *Journal of the History of Biology* 283-316.

Pearson, E.S. “Studies in the history of probability and statistics. XIV Some incidents in the early history of biometry and statistics, 1890-94” (1965) 52 *Biometrika* 3-18.

Prabhakar, Salil *et. al.,* “Biometric Recognition: Security and Privacy Concerns”, (2003) 41 *IEEE Security & Privacy* http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1193209&tag=1 (18/12/2012)

Simon Castellano, Pere, "Los límites jurídico-constitucionales de la Administración electrónica en España y el Open government" (2011) 27 *Revista Aranzadi Derecho y Nuevas Tecnologías* 67.

Tor-Inge, Harbo, “The function of the Proportionality Principle in EU Law” (2010) 6(2) *European Law Journal* 158-185.

Tupman, W.A, “Cross-National Criminal Databases: The ongoing search for safeguards”, (1995) 4(3) *Information & Communication Technology Law* 261-275.

Umpress, D. and Williams, G. “Identity Verification through Keyboard Characteristics” (1985) 23 *International Journal of Man-Machine Studies* 263-273.

Uthmani, Omair*, et. al.,* “Crime risk evaluation within information sharing between the police and community partners”, (2011) 20(2) *Information & Communication Technology Law* 57-81.

Van Der Ploeg, Irma, “Biometrics and Privacy: A note on the politics of theorizing technology” (2003) 6 *Information, Communication & Society* 85-104.

Van Der Ploeg, Irma, “Genetics, biometrics and the informatization of the body” (2007) 43(1) Ann Ist Super Sanità 44-50.

Vega García, Pedro de “Significado constitucional de la representación política” (1985) 44 *Revista de Estudios Políticos* 53-74.

Vega García, Pedro de “El principio de publicidad parlamentaria y su proyección constitucional” (1985) 43 *Revista de Estudios Políticos* 45-66.

Warren, Samuel D and Brandeis, Louis D. “The Right to Privacy” (1980) IV(5) *Harvard Law Review* 1-23, http://www.estig.ipbeja.pt/~ac_direito/privacy.pdf (18/12/2012)

Wein, Lawrence M., and Baveja, Manas, “Using fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology Program” 2005 102(21) *Proceedings of the National Academy of Sciences of the United States of America* 7772-7775.

Weldon, W.F.R., “Mendel's Laws of Alternative Inheritance in Peas” (1902) 2(1) *Biometrika* 228-254.

Westin, Alan, “Science, Privacy and Freedom: Issues and Proposals for the 1970’s” (1966) 66(7) *Columbia Law Review* 1003-1050.

Zagaris, Bruce and Aguilar, Álvaro, “Enforcement of Intellectual Property Protection Between Mexico and the United States: A Precursor of Criminal Enforcement for Western Hemispheric Integration?” (1994) 1(5) *Fordham Intellectual Property, Media and Entertainment Law Journal* 42-123.

NEWSPAPERS/MAGAZINES

Editorial, “Intensifican búsqueda de migrantes desaparecidos” *La Gente* (Mexico online), 24 December 2010 http://www.rlp.com.ni/noticias/90585/intensifican-busqueda-de-migrantes-desaparecidos-en-mexico (20/12/2012)

Editorial, “Migrantes, 72 muertos de fosa en Tamaulipas” *El Universal* (Mexico), 25 August 2010 http://www.eluniversal.com.mx/notas/704017.html (20/12/2012)

Europa Press, “Protección de Datos estará ‘especialmente atenta’ a la posible incorporación de datos nuevos en el DNI electrónico” (Media Release, 1 December 2005) http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2005/common/Interbusca.1_de_diciembre_de_2005.pdf (19/12/2012)

Instituto Nacional de Migración, “Consolida INM simplificación de trámites migratorios”, (Press Release, 7 September 2011) http://www.inm.gob.mx/index.php/blog/show/Consolida-INM-simplificaci%C3%B3n-de-tr%C3%A1mites-migratorios.html (22/12/2012)

Interpol, “Mexico to link its databases with INTERPOL’s in unique new partnership” (Media Release, 3 June 2008) http://www.interpol.int/News-and-media/News-media-releases/2008/N20080603 (21/12/2012)

Mackey Neil, “Blair's DNA crime database plan 'dangerous and flawed'”, *Sunday Herald*, (Glasgow, United Kingdom), 3 September 2000. http://www.shirleymckie.com/documents/Herald3.9.00.pdf (17/12/2012)

Otero, Silvia, “Conectarán Plataforma México con Interpol”, *El Universal*, Mexico City, 10 de junio de 2008 http://www.eluniversal.com.mx/notas/513761.html (21/12/2012);

Speech Technology Center, “World’s first nationwide Voice Identification System deployed in Mexico by Speech Technology Center (Russia)” (Media Release, 4 June 2010) http://speechpro.com/media/news/2010-06-03 (21/12/2012)

Steria, “Steria successfully launches the second generation Schengen Information System for the European Commission (SIS II)” (Media Release, 8 July 2013) http://www.steria.com/media/press-releases/press-releases/article/steria-successfully-launches-the-second-generation-schengen-information-system-for-the-european-comm/ (11/09/2013)

INTERNET SOURCES

"Sir Francis Galton", Galton.org http://galton.org/ (14/01/2013)

Australia, CrimTrac http://www.crimtrac.gov.au/about_us/index.html (21/12/2012)

Australian Government, Department of Immigration and Citizenship, *Managing Australia Borders* http://www.immi.gov.au/managing-australias-borders/border-security/air/airlines/app-checkin.htm (22/12/2012)

Chelowinsky, Ryszard, *Borders and discrimination in the European Union*, ILPA-Immigration Law Practicioners' Association (2002). http://www.ilpa.org.uk/data/resources/13281/ilpa_mpg_borders.pdf (22/12/2012)

Clarke, Mick and Sorensen Steffen, "REALME, Technology Solution Overview" (2012) http://kantarainitiative.org/confluence/download/attachments/45059378/NZ+RealMe+Solution+Overview+v1.pdf (19/12/2012)

Council of Europe legal instruments website http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (23/12/2012)

European Court of Human Rights http://www.echr.coe.int/ECHR/homepage_en (23/12/2012)

Gus Hosein, *Privacy International was founded in 1990 and was the first organization to campaign at an international level privacy issues* (30 March 2004) Privacy International https://www.privacyinternational.org/blog/open-letter-to-un-agency-on-dangers-of-biometric-passport-standard (20/12/2012)

Inter-American Court of Human Rights http://www.corteidh.or.cr/index.cfm?&CFID=1489195&CFTOKEN=37930864 (23/12/2012)

International Organization for Migration (IOM) http://www.iom.int/cms/en/sites/iom/home/about-iom-1/mission.html (20/12/2012)

Interpol counterfeit payment cards http://www.interpol.int/Crime-areas/Financial-crime/Payment-cards (21/12/2012)

Interpol data exchange http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-link (20/12/2012)

Interpol FAST and efficient international disaster victim Identification http://www.interpol.int/INTERPOL-expertise/Databases/FASTID/FAST-and-efficient-international-disaster-victim-IDentification (21/12/2012)

Interpol fusion task force website http://www.interpol.int/Public/FusionTaskForce/default.asp (21/12/2012)
Interpol overview website http://www.interpol.int/INTERPOL-expertise/Overview (21/12/2012)

Korff, Douwe, "Comparative Study on Different Approach to New Privacy Challenges, in Particular in the Light of Technological Developments" (2010). http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf (23/12/2012)

Korff, Douwe, "EC Study on Implementation of Data Protection Directive 95/46/EC" (2002). Available at http://ssrn.com/abstract=1287667 (23/12/2012)

Kuner, Christopher, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", *Tilbrug Institute for Law, Technology and Society, (*2010) http://dx.doi.org/10.2139/ssrn.1689483 (23/12/2012)

Mexico, Federal Institute for Access to Public Information and Data Protection http://www.ifai.org.mx/English (23/12/2012)

Mexico, National Institute of Migration (INM) http://www.inm.gob.mx/index.php/page/pagina_principal/en.html (20/12/2012)

New Zealand, Customs service website http://www.customs.govt.nz/features/bordersector/transtasmantravel/Pages/default.aspx (20/12/2012)

New Zealand, immigration area of responsibility http://www.dol.govt.nz/about/responsibilities/ (22/12/2012)

New Zealand, immigration website http://www.immigration.govt.nz/ (22/12/2012)

New Zealand, National DNA databank
http://www.esr.cri.nz/competencies/forensicscience/dna/Pages/DNAdatabank.aspx (21/12/2012)

New Zealand, New IT system for Immigration New Zealand http://www.immigration.govt.nz/migrant/general/generalinformation/newitsystems/ (20/12/2012)

Spain, Data Protection Spanish Agency http://www.agpd.es/portalwebAGPD/index-ides-idphp.php (19/12/2012)

Spain, General Minister for Migration and Immigration http://extranjeros.mtin.es/es/Organizacion/ (20/12/2012)

USA, National Institute of Standards and Technology http://www.nist.gov/itl/iad/ig/ansi_standard.cfm (22/12/2012)

SEMINAR/BACKGROUND PAPERS

Darwish, Jamil “International efforts against currency & security document counterfeiting” (Paper presented at the Tenth ID World International Congress, Milan, 3 November 2011)

Downes, Garry, “The relationship between reasonableness, proportionality and merits reviews in Australia”, (Paper presented at New South Wales Young Lawyers Seminar Issues of Administrative Law, Sydney, 24 September 2008)

Hunter, L., Orr, A. and White, B., “Towards a framework for promoting financial stability”, (Paper presented at The Institution of Professional Engineers New Zealand, Wellington, 22 March 2006)

International Organization for Migration, “International Terrorism and Migration”, *Background Paper*, Immigration and National Security, (2003), 16 http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/activities/tcm/Int_terrorism_migration.pdf (20/12/2012)

Nick Nugent, “High Security Identification Documents Using QSDC to Determine the Right Mix” (Paper presented at the Tenth ID WORLD International Congress, in Milan, 4 November 2011)

Wing, Bradford, “Future of ID, Developments in Standards & Critical Projects”, in Wise Media, (Paper presented at the Tenth ID World International Congress, Milan, 3 November 2011)

APPENDICES

APPENDIX A

NATIONAL PROFILES TABLE

	Australia	Mexico	New Zealand	Spain
Capital	Canberra	Mexico City	Wellington	Madrid
Population	22,683,600[1]	112 336 538[2]	4,453,062[3]	46,815,916[4]
Area (sq km)	7,692,024	1,964,375	268,680	505,988
Major Language	English	Spanish	English	Spanish
Currency	Australian Dollar	Mexican Peso	New Zealand Dollar	Euro
Ethnic Groups	European 92% Asian 7% Aboriginal and other 1%	Mestizo[5] 60%, Indigenous 30%, European 9%, other 1%	European 69.8%, Maori 7.9%, Asian 5.7%, Pacific islander 4.4%, other 0.5%, mixed 7.8%, unspecified 3.8%	composite of Mediterranean and Nordic types
Government Type	Parliamentary democracy	Federal democracy	Parliamentary democracy	Parliamentary monarchy
Administrative Divisions	6 states and 2 territories	31 states and 1 federal district	16 regions and 1 territory	17 autonomous communities and 2 autonomous cities
Constitution	1900 Constitutional Monarchy	1917 Constitutional Republic	1986 Constitutional Monarchy	1978 Constitutional Monarchy
Legal System	Common Law	Civil Law	Common Law	Civil Law
Suffrage	18 years of age; universal and compulsory	18 years of age; universal and compulsory[6]	18 years of age; universal	18 years of age; universal
Branches	Executive, Legislative and Judicial	Executive, Legislative and Judicial	Executive, Legislative and Judicial	Executive, Legislative and Judicial
GDP[7]	3.4	3.9	3.0	-1.4

[1] Australian Bureau Statistics, at the end of June 2012 http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0 (18/01/2013)
[2] Instituto Nacional de Estadistica y Geografia (Mexico), results of the last national census in 2010 http://www.inegi.org.mx/default.aspx (18/01/2013)
[3] Statistics New Zealand http://www.stats.govt.nz/ (11 October 2010)
[4] Instituto Nacional de Estadistica (Spain), result of the last national census http://www.ine.es/censos2011_datos/cen11_datos_inicio.htm (18/01/2013)
[5] A traditional term used to denote people of combined indigenous and Spanish ancestries.
[6] But not enforced.
[7] GDP growth (annual %) data obtained from the World Bank http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG/countries?display=default (18/01/2013)

APPENDIX B

BIOMETRICS TYPOLOGY

1. *Physical Characteristics.* In this section, the discussion revolves around the most common or popular physical biometric characteristics: the chemical composition of the body, thermal emissions, iris and retina patterns, fingerprints, palmprints, hand geometry, face and skin pores.

The human body is made of different types of cells, tissues, muscles and organs, and every part of the human body can be measured[1]. The most popular measures for biometric systems are the following:

a) *Chemical composition of body.* Individual odours have been exploited for long time. The best example of this is the use of dogs to track people. Biometric systems can measure the concentration of personal odour[2].

b) *Thermal emissions.* Biometric thermal emissions are images of parts of the body in the short, mid or long infrared wavelengths. The resulting images, however, are not rich in grey values[3].

c) *Iris and retina patterns.* The features of the eyes can be easily measured[4]. Since 1986, the iris has been used for identification. The development of an iris prototype unit by the American Defence Nuclear Agency began in the 1990s, but it was not until 1995 that the iris prototype became available as a commercial product[5]. Retina recognition seeks to identify a person by comparing images of the blood vessels in the back of the eye, also known as the choroidal vasculature[6]. Simon and Goldstain worked out blood vessel

[1] Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, (W.H. Freeman and Company, 1973); Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*"* (1999) 13(3) *International Review of Law, Computers & Technology* 337-363; Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000); Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003); Bolle, Ruud M., *et. al*., *Guide to Biometrics*, (Springer, 2003).

[2] Personal odour is susceptible to all types of influences, from diet and state of health to the use of soaps, perfumes and deodorants. It is not yet clear whether these factors can be normalized well enough to allow the reliable identification of individuals. Bolle, Ruud M., *et. al*., *Guide to Biometrics*, above n 1, pp. 58-59.

[3] Infrared spectral resolution is measured by the numbers of bands, their width and their range within the electromagnetic spectrum. This works because skin is a better thermal conductor that air and thus contact with the ridges causes a noticeable drop in temperature on a heated surface. The technology claims that optical scanners can overcome dry and wet skin tissues and can sustain a higher static discharge. Ibidem, p. 33.

[4] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, pp. 28-31; Wayman, James, *et. al*., *Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1.

[5] Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, above n 1, p. 71-130; Wayman, James, *et. al*., *Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 9.

[6] Bolle, Ruud M. e*t. al.*, *Guide to Biometrics*, above n 1, p. 53.

pattern measurements and retina recognition has been developed commercially since the mid-1970s.

d) *Fingerprints.* Fingerprint identification is the process of comparing given and known skin ridge impressions from fingers to determine if the impressions are from the same finger, thus identifying or verifying the owner of a given fingerprint. Fingerprint identification is the most widespread biometric systems. It has been widely used in personal identification for several centuries[7], and still is largely used in law enforcement applications. However, recent combinations of factors favour the use of fingerprints for a much larger market of personal authentication[8]. In 1984, the Federal Bureau of Investigation (FBI) began pushing to develop an automated fingerprint identification system. The Integrated Automated Fingerprint Identification System (IAFIS), the FBI's large-scale ten fingerprints identification system, has since become operational[9].

e) *Palmprints.* Palmprints, as well as fingerprints, are still considered one of the most reliable means of distinguishing a man from his fellows because of their stability and uniqueness. The palm of the hand, flexure lines or finer lines, are used mainly to foretell the future, as well as to diagnose diseases. Palmprint recognition implements many of the same matching characteristics of fingerprint recognition[10].

f) *Hand geometry.* The geometric shape of the hand is not descriptive enough for identification[11]. Unlike fingerprints, the shape of the human hand is not unique. However, for purposes of verification, hand geometry data can be very useful and easier to collect. In 1974, the first commercial hand geometry systems became available. Therefore, in 1980, the U.S. Army began testing hand geometry for use in banking. During the 1990s, major public use of hand geometry occurred at the Olympic Games where hand geometry systems were implemented to control and protect physical access to the Olympic Village in Atlanta[12].

---

[7] For further details, see Section 2.4.1. Definition Biometry or Biometrics?

[8] The structural traits of the ridges in the centre fingerprint area basically classify fingerprint patterns. Familiar fingerprint patterns are divided into six main classes: arch, tented arch, right loop, left loop, whorl and twin loop. Some patterns are not included because they occupy a very small proportion and are known as special patterns. Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, pp. 88; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1.

[9] Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, above n 1, p. 71-130; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al*, *Biometrics, Theory, Methods, and Applications*, above n 1.

[10] There are usually three principal lines made by flexing the hand and wrist in the palm, which are named the heart line, the head line and the life line. Palm biometrics is represented by the information presented in a friction ridge impression. This information combines the ridge flow, ridge characteristics and ridge structure of the raised portion of the epidermis. The data represented by these impressions allow the identification or authentication of individuals by comparing them with a database. Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, pp. 111; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1, p. 58.

[11] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, pp. 34.

[12] Woodward, John D. Jr. *et. al*., *Biometrics, Identity Assurance in the Information Age*, above n 1, p. 71-130; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation,* above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1.

g) *Face.* Faces are rich in information about an individual's identity; it provides information on race and sex, as does the distance between various facial features like the eyes, cheeks, nose, eyebrows, for example. The face can also tell about an individual's mood and mental state. Among all the biometric identification systems, facial recognition has attracted much attention in recent years because of its potential as the most non-intrusive[13]. Therefore, facial recognition has become one of the most researched. In the 1960s, Bledsoe developed the first semi-automated facial recognition system under contract for the U.S. government[14]. However, it was not fully automated as it required a system administrator to locate useful features such as the eyes, ears, nose and mouth on photographs. By the 1970s, facial recognition took another step towards automation, but the problem was that measurements and locations had to be computed manually[15]. Then in 1988, the Lakewood Division of Los Angeles County Sheriff's Department began using a facial recognition system and deployed a suspect to conduct a database search of criminals whose features had been digitized. Furthermore, an Eigenface technique was developed for face recognition[16]. In the 2000s, face recognition was used at the Super Bowl in Tampa, Florida. The International Organization for Standardization (ISO) established the ISO/IECJTC1 subcommittee 37 (JTC1/SC37) to assist in the standardization of generic biometric technologies[17]. The ICAO employed face recognition technology as mandatory features for travel documents[18].

h) Pores of the skin. Sweat pores have been used to assist in forensic matching. Although most matching methods have emphasized minutia comparisons and used pores as ancillary comparison features, the ability to match prints based on pore information alone has been documented[19]. Considerable research has shown that pores do not disappear, move or spontaneously generate over time, which is the basis for them to be considered a biometric feature.

2. *Behavioural Characteristics.* In this section, behavioural characteristics will be explained along with the most common or popular behavioural measures: handwritten signatures, voice, keystrokes and gait.

Behavioural biometrics are learned or acquired over time and are dependent on one's state of mind or even subject to deliberate alteration. There are two kinds of behaviours: innate

[13] Face recognition systems contains two key steps, which are face detection and location together with features extraction and face recognition. The first step decides whether the input images or image sequences include faces, and if they do, figure out the position of the faces, then the segments each face from background. The second step looks for face features which distinguish individuals, and judges whether the individual in image is the given person or whether he or she is in database. Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, p. 27 and 137; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V*., et. al*., *Biometrics, Theory, Methods, and Applications*, above n 1.

[14] Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, above n 1, Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V*., et. al*., *Biometrics, Theory, Methods, and Applications*, above n 1.

[15] Idem.

[16] Idem.

[17] Idem.

[18] For further details, see Chapter 4. Biometric Systems in the Context of Transborder Immigration Flow

[19] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, p. 31-34; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1.

and learned. The innate behaviour is determined by inherited pathways of nervous coordination. On the other hand, learned behaviour becomes more or less permanently altered as a result of the individual way of life, as well as social and cultural experiences[20].

The specialised literature highlights that the voice and handwritten signature are the most widespread behavioural characteristics. In addition, keystroke and gait are other important behavioural characteristics that are still in the testing and development stage.

a) *Handwritten signature.* The handwritten signature is one of the most widespread ways of verifying an individual's identity in daily operations. The design of a signature system is based on the fact that people do not write according to a standard type of penmanship and deviation from the norm is dependent on the individual. The signature was in service before the advent of computers and has seen wide usage in document authentication and transaction authorization in the form of checks and credit card receipts. In 1965, North American Aviation developed the first signature recognition system[21].

b) *Voice.* Voice is one of a person´s most distinguishing attributes. Voice is a convenient and natural tool for human communication. It is possible to identify people by merely hearing their voices. Even language does not matter; emotional state, health, aging and speaking habits (rhythm and intonation) do not affect the voice[22]. In 1976, the first prototype system for voice recognition was developed. The following year, Veripen Inc., of New York, was awarded a patent for a "personal identification apparatus". This device made it possible to digitally capture of dynamic characteristics of an individual's signature characteristics. Since 1980, the National Bureau of Standards (NBS) developed the NBS Speech Group to study and promote the use of speech processing techniques[23].

c) *Keystrokes.* Biometric keystroke is the identification of a person by their personal typing style. So far, keyboard characteristics are rich in cognitive qualities and hold promise as an individual identifier. When a computer user types on a computer keyboard, a digital signature is left in the form of keystroke latencies[24]. Zhang explains that: "[e]xperiment for keystroke characterization showed that a high degree of correlation could be obtained if the same person typed both the reference keystroke and the test ones"[25].

---

[20] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, p. 39.

[21] The motion of a pen on paper, resulting from muscle contraction-relaxation, leaves a partial trace of the trajectory of the pen tip. Ibidem, p. 203; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1.

[22] The vocal tract is generally considered the speech production organ above the vocal folds, which consists of the laryngeal pharynx, oral pharynx, oral cavity, nasal pharynx and nasal cavity. The vocal tract modifies the spectral contents of an acoustic wave as it passes through the tract, thereby producing the voice. An acoustic wave is produced when the airflow from the lungs is carried by the trachea through the vocal folds. Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1, pp. 48-49; Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1, p. 18-182; Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1.

[23] Idem.

[24] The common use keystroke measures are inter-key times and hold times. The inter-key times means inter-character time intervals measured as user types. Hold times represent the time duration between the moments every key button is hit to the moment it is released. Both features can be obtained by computer programming. Umpress, D. and Williams, G. "Identity Verification through Keyboard Characteristics" (1985) 23 *International Journal of Man-Machine Studies* 263-273.

[25] Zhang, David D. *Automated Biometrics Technologies and Systems,* above n 1*,* pp. 229-230.

d) *Gait.* Using gait as a biometrics has recently attracted interest. People need to walk, so their gait is usually apparent and hard to disguise. It requires no subject contact. Gait biometrics involves its derivation by computer vision, for this only way it can satisfy its purpose. Some insight into gait as a biometrics can be drawn from psychology[26]. The strength of gait recognition lies in its applicability to recognizing people at distance in video images. Initial work has been carried out on identifying people by gait using motion capture equipment such as moving light displays or special markers[27].

[26] Ibidem, p.254; Wayman, James*, et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1.

[27] Bolle, Ruud M., *et. al*., *Guide to Biometrics*, above n 1, p. 55.

APPENDIX C.

HOW BIOMETRIC SYSTEMS WORK

1. Authentication (verification) biometric system. In order to understand the use of biometric systems, it is important to know how authentication biometric systems work.

Specialised literature considers fingerprints, palmprints, voice or iris as the best physical characteristics for authentication biometric systems. Authors explain that biometric systems are used to verify are designed to ask the question "Am I the person I claimed to be? (Am I who I say I am?)" In special cases, many different types of measurements can be involved at the same time; these are the combined biometric systems[1].

In a verification system, it is not necessary to have a database since the objective of such a system is to verify a person's identity, which means the registered pattern is displayed when a comparison is conducted[2]. Zhang and Hopkins explain the verification process in the following steps[3]:

- ✓ The person being checked enters a password or swipes his/her identification card.
- ✓ The system captures his/her biometrics feature(s).
- ✓ The captured data is processed and compared with the one associated with the password or identification card.
- ✓ The system gives a verification result.
- ✓ The answer could be "Yes, s/he is" or "No, s/he is not."

2. Identification (recognition) biometric system. In order to understand the use of biometric systems, it is important to know how authentication biometric systems work.

The literature considers face recognition the best feature for recognising people at a distance without their knowledge or cooperation[4]. Authors explain that biometric systems that are used to identify are designed to ask the question "Who am I?" A biometric identification system works by comparing a scanned biometric against a database of

---

[1] Sokal, Robert and James, Rohlf, *Introduction to Biostatistics*, (W.H. Freeman and Company, 1973); Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*"* (1999) 13(3) *International Review of Law, Computers & Technology* 337-363; Zhang, David, *Automated biometrics: technologies and systems,* (Kluwer Academic Publishers, 2000); Wayman, James, *et. al., Biometric Systems Technology Design and Performance Evaluation*, (Springer, 2005); Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, (IEEE and WILEY, 2010); Woodward, John D. Jr. *et. al.*, *Biometrics, Identity Assurance in the Information Age*, (McGraw Hill Osborne, 2003); Bolle, Ruud M., *et. al*., *Guide to Biometrics*, (Springer, 2003).

[2] Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1.

[3] Idem; Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*",* above n 1.

[4] Wayman, James*, et. al., Biometric Systems Technology Design and Performance Evaluation*, above n 1; Boulgouris, Nikolaos V., *et. al.*, *Biometrics, Theory, Methods, and Applications*, above n 1; Bolle, Rudd M., *Guide to Biometrics*, above n 1; Zhang, David D., *Automated Biometrics Technologies and Systems,* above n 1*;* Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*",* above n 1.

biometric information. A biometric-based identity system can ensure that a person has one and only one identity in the database[5].

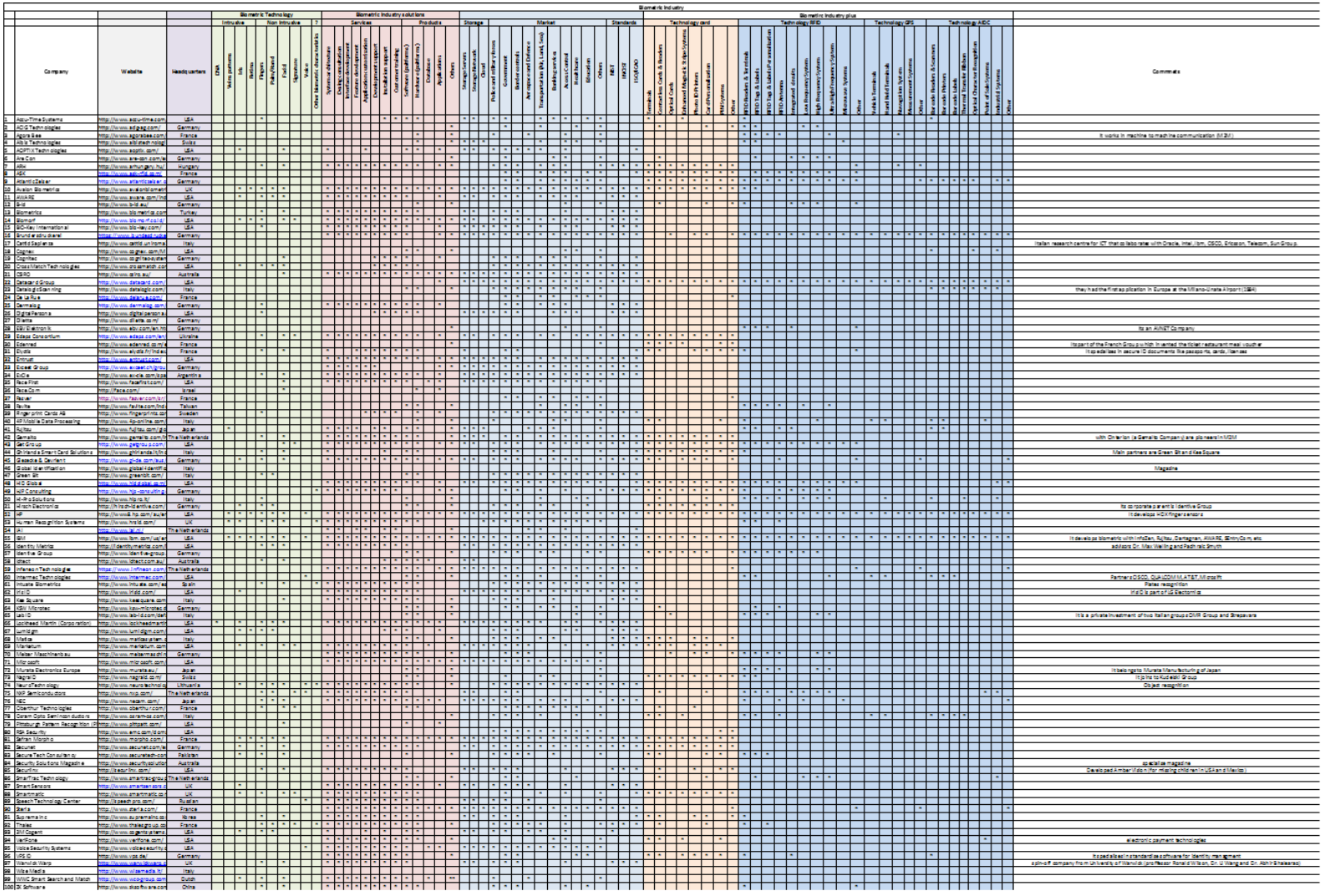
In an identification system, a huge database is used to store hundreds of thousands of people's digital biometric features[6]. According to Zhang and Hopkins, the identification process is as follows[7]:

- ✓ The system gives a result whether the person being checked is registered or not.
- ✓ The answer could be "Yes, s/he is" or "No, s/he is not."

Hopkins notes that when dealing with small numbers of people, unique identity can be established by manual processes. However, when dealing with millions of people, totally automated biometric systems must provide a fast and explicit "yes/no" answer to the question "Is this person already enrolled in this system?" Ideally, no human experts are required[8].

[5] Idem.
[6] Zhang, David D., *Automated Biometrics Technologies and Systems*, above n 1, p. 11;
[7] Idem; Hopkins, Richard, "An introduction to biometrics and large scale civilian identification*",* above n 1.
[8] Idem.

Appendix D. List of Companies in the Biometric Industry (Complete Table)



| | Company | Website | Headquarters | Biometric Technology: Intrusive: DNA | Voice patterns | Iris | Retina | Face | Odor/Smell | Facial | Signature | Keystroke | Other Biometric characteristics | Biometric Industry solutions: Services: Systems Integration | Data consolidation | Biometric Development | Consulting | Application customization | Development support | Installation support | Outsourced hosting | Products: Software (platforms) | Hardware (platforms) | Database | Application | Others | Biometric Industry: Storage: Storage Servers | Storage Network | Client | Risk and offline claims | Government | Border controls | Aerospace and Defense | Transportation (Air, Land, Sea) | Banking and e-commerce | Access Control | Healthcare | Education | Others | NIST | ANSI | ISO/IEC JTC1 | Standards | Technology card: Terminals | Contact Less Cards & Readers | Contact Cards | Combined Magnetic Stripe Systems | Photo ID Printers | Card Personalization | RFID systems | Other | Technology RFID: RFID Readers & Terminals | RFID Tags & Labels | RFID Tags & Labels Pre-personalization | RFID Antenna | Integrated circuits | Low frequency System | High frequency System | Ultra-high Frequency System | Microwave Systems | Other | Technology GPS: Vehicle Terminals | Hand Held Terminals | Navigation System | Measurement Systems | Other | Technology AIDC: Barcode Readers & Scanners | Barcode Printers | Barcode Labels | Mobile Computers | Machine Vision | Optical Character Recognition | Point of Sale Systems | Industrial Systems | Other | Comments |
|---|---|---

APPENDIX E.

EURODAC INTRODUCTORY INFORMATION

Eurodac is a transnational database containing the personal and biometric information of all asylum seekers and illegal immigrants found within the European Union (EU)[1]. Eurodac contains personal information like country of origin, sex, and date and place of apprehension or asylum application. It includes the fingerprints of asylum applicants and illegal immigrants over the age of 14, thus allowing authorities to determine whether individuals have already applied for asylum in another EU Member State or have transited illegally through another EU Member State. According to the European Commission, asylum data stored in member States' national databases have already been instrumental in solving cases of terrorism and serious crimes committed in other member States.

In 2009 and 2010, the European Commission presented a proposal to expand the use of Eurodac database for terrorism and serious crimes. However, the European Data Protection Supervisor (EDPS) argued that the need and proportionality of law enforcement access to EURODAC data has not been sufficiently demonstrated, shifting to the wholesale sharing of biometric information in EURODAC which requires more than just anecdotal evidence as justification[2]. The potential for error in matching fingerprints and the resulting implication of innocent asylum seekers in crimes they did not commit has been pointed at by the UN High Commissioner for Refugees (UNHCR), who recommends strengthening provisions prohibiting the transfer of information about asylum seekers or refugees to third countries[3].

[1] *Council Regulation (EC) No 2725/2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin,* [2000] OJ L 316/15.

[2] European Data Protection Supervisor "Opinion to the European Parliament on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…]".https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/2012-09-05_edps_opinion_on_eurodac.pdf (24/12/2012)

[3] UNHCR "Comments to the European Parliament on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…]" http://www.unhcr.org/50adf9749.pdf (24/12/2012)

APPENDIX F.

SCHENGEN INFORMATION SYSTEM

Note: The information provided in this appendix is a summary of the Schengen area and cooperation website[1].

In 1985, an agreement was signed at Schengen (a town in Luxemburg) for the purpose of creating a free movement area that extends throughout the territories of the contracting parties while at the same time maintains a high level of security for their citizens. More freedom in movement, however, implies rather higher risks than better security. In meeting these two a priori contradictory objectives, the Convention Implementing the Schengen Agreement introduced a series of compensatory measures, which include:

- Stricter controls at external borders,
- A common policy for granting visas,
- Closer cooperation between police, judiciary and customs,
- A common policy for asylum,
- A common policy on narcotic drugs and psychotropic substances,
- A common policy on firearms and ammunition and
- Setting up the Schengen Information System.

The signatory States to the agreement have abolished all internal borders in lieu of a single external border. Here, common rules and procedures are applied with regard to visas for short stays, asylum requests and border controls. Simultaneously, to guarantee security within the Schengen area, cooperation and coordination between police services and judicial authorities have been stepped up.

Schengen cooperation has been incorporated into the European Union (EU) legal framework with the Treaty of Amsterdam of 1997. However, all countries cooperating in Schengen are not parties of the Schengen area. This is either because they do not wish to eliminate their border controls or because they do not yet fulfil the required conditions for the application of the Schengen *acquis.*

The first agreement between the five original group members was signed on 14 June 1985. A further convention was drafted and signed on 19 June 1990. When it took effect in 1995, it abolished checks at the internal borders of the signatory States and created a single external border where immigration checks for the Schengen area are carried out in accordance with identical procedures. Common rules regarding visas, the right of asylum and checks at external borders were adopted to allow the free movement of persons within the signatory States without disrupting law and order.

Accordingly, in order to reconcile freedom and security, this freedom of movement was accompanied by so-called "compensatory" measures. These involved improving cooperation and coordination between the police and the judicial authorities in order to safeguard internal security and, specifically, to fight organised crime. With this in mind, the Schengen

1 http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm (24/12/2012)

Information System (SIS) was set up. The SIS is a sophisticated database used by authorities of the Schengen member countries to exchange data on certain categories of people and goods.

The SIS allows national border control and judicial authorities to obtain information on persons or objects. Member States supply information to the system through national networks (N-SIS) connected to a central system (C-SIS). This IT system is supplemented by a network known as SIRENE (Supplementary Information Request at the National Entry), which is the human interface of the SIS.

The Schengen area gradually expanded to include nearly every Member State. Italy signed the agreements on 27 November 1990; Spain and Portugal joined on 25 June 1991; Greece followed on 6 November 1992, then Austria on 28 April 1995 and Denmark, Finland and Sweden on 19 December 1996. The Czech Republic, Estonia, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia and Slovakia joined on 21 December 2007 and the associated country Switzerland on 12 December 2008. Bulgaria, Cyprus and Romania are not yet fully-fledged members of the Schengen area; therefore, border controls between these countries and the Schengen area are in place until the EU Council decides that the conditions for abolishing internal border controls have been met.

- *The second-generation Schengen Information System (SIS II)*

As the SIS has been operational since 1995, work is in progress on a new system based on new technology with enhanced functionalities. This new system (SIS II) is currently undergoing extensive tests in cooperation with member States.

The Council adopted two legislative instruments on 6 December 2001: Regulation (EC) No 2424/2001 and Decision 2001/886/JHA, making the Commission responsible for developing SIS II and providing for the related expenditure to be covered by the general EU budget. These instruments were modified in 2006, extending the period of their validity to 31 December 2008.

The Commission published a communication [COM (2001) 720] on 18 December 2001, examining ways to create and develop SIS II. Following studies and discussions relating to the architecture and functionalities of the future system, the Commission presented three proposals for legislative instruments in 2005. Two of the instruments in this package (Regulation (EC) No. 1987/2006 on first pillar aspects of the establishment, operation and use of SIS II and Regulation (EC) No. 1986/2006 on access to SIS II by the services responsible for issuing vehicle registration certificates) were adopted on 20 December 2006. The third instrument (Decision 2007/533/JHA determining third pillar aspects of the establishment, operation and use of SIS II) was adopted on 12 June 2007.

The Justice and Home Affairs Council of December 2006 endorsed the SISone4all project (a joint effort among member States coordinated by Portugal). SISone4all was a temporary solution, which enabled nine EU member States that joined the EU in 2004 to connect to the current SIS system (SIS1+) with some technical adjustments. The successful completion of SISone4all, in conjunction with positive Schengen evaluations, allowed for the lifting of internal border controls along land and sea borders with these new countries by the end of 2007 and for air borders in March 2008.

Lifting internal border controls paved the way for implementing alternative and less risky approaches for migrating from SIS I + to SIS II. Following requests made by member States

to allow more time to test the system and adopt a less risky strategy for migration from the old system to the new one, the Commission presented proposals for a regulation and a decision was made to define the tasks and responsibilities of the various parties involved in preparing for the migration to SIS II (including testing and any further development work needed during this phase). These proposals were adopted by the Council on 24 October 2008.

APPENDIX G.

PRÜM CONVENTION

Note: The information provided in this appendix is a summary of the Schengen area DNA cooperation website[1].

In 2005, at Prüm (a town in Germany), seven European Union (EU) members States signed the Treaty of Prüm on stepping up cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration. The aim of this decision is to intensify cross-border police and judicial cooperation between (EU) member States in criminal matters so as to improve the exchanges of information between the authorities responsible for preventing and investigating criminal offences. The decision sets out provisions with regard to:

1. Automated access to DNA profiles, dactyloscopic data and certain national vehicle registration data;
2. Supply of data in relation to major events;
3. Supply of information in order to prevent terrorist offences;
4. Other measures for increasing cross-border police cooperation.

- *The Establishment of National Databases and Automated Access To Data*

EU member States are to establish national DNA analysis files for the purpose of investigating criminal offences. The reference data, consisting of the non-coded part of the DNA and a reference number that does not enable an individual to be identified, must be made available to other EU member States to carry out automated searches. These searches are performed via national contact points by comparing DNA profiles, but only in individual cases and on a hit/no-hit basis. If the search provides a match, the national contact point carrying out the search receives the reference data electronically. If no profile is found for the specific individual under investigation or against whom criminal proceedings have been brought, the requested EU member Sate may be obliged to establish a DNA profile for that individual.

EU member States must also make available reference data from the national automated fingerprint identification systems (AFIS). For this purpose, reference data will consist only of dactyloscopic data and a reference number. Searches are carried out by comparing dactyloscopic data and, like DNA searches, only in individual cases on a hit/no-hit basis. Confirmation of the match is conducted by the national contact point of the requesting EU member State. Supplying further available personal data for matching DNA or dactyloscopic data and other information relevant to the reference data is governed by national law, including the Mutual Legal Assistance (MLA) in the requested EU member States.

The national contact points are also given access to certain national vehicle registration data via automated online searches. These searches may only be conducted with a full chassis or registration number.

---

1 http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_en.htm (24/12/2012)

- *Supply of Information to Fight Terrorism*

For the purpose of preventing terrorist activities, but only in individual cases and to the extent required by the conditions leading to the supposition that criminal offences will be committed, EU member States may provide the following data to each other via the national contact points:

1. Surname and first names;
2. Date and place of birth;
3. A description of the conditions leading to the supposition that criminal offences will be committed.

The country providing this data may impose certain binding conditions on the receiving country for the use of said data.

- *Other Measures for Enhancing Cross-Border Police Cooperation*

EU member States may effectuate joint patrols and other joint operations to prevent criminal offences and to maintain public order and security in a given EU member State's territory. In such cases, designated officers and officials from the seconding country participate in the host country's operations. The seconding officers may be conferred executive powers or may be allowed to exercise their executive powers, but only under the guidance and in the presence of the host officers. The competent authority of the host country is responsible for the control of the actions of the seconding officers.

With regard to mass gatherings and other comparable major events, disasters and serious accidents, EU member States are to provide mutual assistance to each other. This assistance should consist of information exchanges, the coordination of police measures and the contribution of material and physical resources.

An EU member State must provide assistance and protection to the other country's officers on duty, equivalent to that provided to its own officers.

- *Provisions on Data Protection*

EU member States must guarantee that the personal data processed in accordance with this decision is protected by national laws. Only the competent authorities may process personal data. They must ensure the accuracy and current relevance of the data. Steps must be taken to rectify or delete incorrect data or data that was supplied when it should not have been. Personal data must be deleted if no longer needed for the purpose it was made available or if the storage restrictions, as provided by national law, has expired.

The relevant authorities must take technical and organisational measures to protect personal data against destruction, loss, unauthorised access, alteration or disclosure. For the purpose of verifying the permissibility of the non-automated processing of personal data, this processing must be logged. Similarly, the automated processing of personal data must be recorded. The independent data protection authorities in EU member States are responsible for the legal examinations of personal data processing.

Any individual has the right to information on the data that has been processed in relation to his or her person, including information on the origin of the data, the recipients of the data,

and the purpose and legal basis for processing the data. The individual may request corrections to or the deletion of inaccurate or unlawfully processed data. If the individual's rights have been violated with regard to data protection, he or she may lodge a complaint with an independent court or tribunal and claim damages or other legal compensation.

APPENDIX H.

NATIONAL IMMIGRATION POLICY

Note: This information is a summary of the national immigration policy of the four countries study.

Australia's Immigration Policy:

Australia has a programme of strict control over migration movements. The Department of Immigration and Citizenship (DIAC)[1] is in charge of the arrival and settlement of migrants in Australia. The Australian immigration is managed by the *Migration Act 1995* and associated regulations.

For Australia, 2008, 2009 and 2013 were important years for reforming their migration legal framework. In January 2009, the government established a new Critical Skills List (CSL) and in April 2009[2], February 2011[3] and December 2012, they announced a series of reforms to the temporary skilled migration program

The Australian migration programme has the following objectives[4]:

1. To implement strategies to strengthen the economic, budgetary and social benefits from both permanent and temporary migration.
2. To implement strategies to promote managed migration and strengthen international cooperative efforts against people smuggling, trafficking in persons and terrorism.
3. To provide effective scrutiny at the border, including by examining passengers and crew and their movement information before their arrival in Australia, as well as examining and confirming their identity and authority to enter Australia upon arrival.
4. To provide identification, verification and biometric matching capabilities across a range of business processes, through the collection of biodata and images, and its integration with alert systems.
5. To implement strategies to promote compliance and prevent and deter non-compliance with immigration law.
6. To locate people who are no longer permitted to stay in Australia and regularise their immigration status including, where necessary, their removal from Australia.
7. To monitor business sponsors for compliance with sponsorship undertakings and, as appropriate, apply sanctions for those in breach and/or refer their cases to other relevant agencies.
8. To continue to manage and process protection visas onshore.
9. To facilitate the effective management of asylum seekers.

The Australian Government determines the number of migrants Australia will accept at the beginning of each financial year. This includes the number of applications Australia will

[1] The Department of Immigration and Citizenship (DIAC) http://www.immi.gov.au/ (20/12/2012)
[2] Australia Government, Department of Immigration and Citizenship, *Annual Report* (2008-2009)
[3] Australia Government, Department of Immigration and Citizenship, *The People of Australia-Australia's Multicultural Policy*, (2011)
[4] Australia Government, Department of Immigration and Citizenship, above n 90.

accept from applicants applying from overseas, as well as applicants applying from within Australia.

The varieties of visa fall into two main categories: *temporary* and *permanent*. There are six main categories of permanent visas: skilled migration, family migration, business migration, employer-sponsored, refugee/humanitarian and special eligibility (former Australian residents). Temporary visas allow people to visit Australia for a limited time for the purposes of tourism, study, work, business, medical treatment or visiting relatives. However, these categories of permanent and temporary visas have approximately 140 visa subclasses with their own sets of eligibility criteria[5].

The significance of this for this thesis is that Australia has set itself the objective of implementing biometrics into their immigration policy. In addition to this, border clearance of airline staff using face recognition comparisons against enrolled templates was used first by QANTAS and the Australian Customs Service.

In 2003, the Australian Customs Service inaugurated a pilot program at Sydney Kingsford Smith Airport, which consisted of enrolling QANTAS staff members on a computerised system that matches video images against respective templates in the project database. This programme is now called SmartGate[6]. SmartGate is a kiosk that checks whether Australian and New Zealand travellers are eligible for self-processing and the gate performs the identity check and clearance. SmartGate is available at Sydney, Adelaide, Brisbane, Cairns, Melbourne, Perth, Gold Coast and Darwin international airports[7].

In 2004, the Department of Immigration and Citizenship (DIAC) was authorised to research and test ways of incorporating biometric technologies into existing visa and entry arrangements, and to find a way of increasing the capacity to store biometric images. Two systems were developed and are now known as the Identity Services Repository (ISR)[8].

In 2008, the Australian National Audit Office examined the DIAC's management of the introduction of biometric systems. The Auditor General pointed out that:

> "DIAC has relatively limited capability to use other biometric data, such as fingerprints for matching purposes. [T]here is a risk that DIAC is unable to benefit fully from interactions with domestic and overseas systems. The current relatively limited fingerprint matching capability leaves the department in a position where it is unable to benefit fully from the international developments tending towards a broader use of fingerprints"[9].

Furthermore, under the *Migration Act 1995* access to, and disclosure of, identifying information does not extend to the third parties on which the DIAC discloses information.

---

[5] The Department of Immigration and Citizenship (DIAC), section visas immigration and refugees http://www.immi.gov.au/immigration/ (20/12/2012)

[6] International Organization for Migration, "International Terrorism and Migration", above n 80; Australia Government, Australian National Audit Office, *Audit Report* No 24 (*2007-2008)*

[7] Australian Customs and Border Protection Service, SmartGate http://www.customs.gov.au/site/page5552.asp (20/12/2012)

[8] Australia Government, Department of Immigration and Citizenship, *Review of Personal Identifier Provisions Introduced In 2004 to Migration Act 1958,* Final Report (2009) 16

[9] Australia Government, Australian National Audit Office, *Audit Report,* above n 94.

"DIAC cannot ensure that there is/will be no inappropriate use or disclosure of identifying information by the agencies to which it discloses the information"[10].

Since October 2009, the DIAC "implemented the Five Country Conference (FCC) (Australia, the United Kingdom, the United States of America, Canada and New Zealand) Secure File Share Server. This provides a secure, electronic means of sharing biometric data"[11].

> "In December 2009, the department commenced collection of biometrics (fingerprints and facial images) from consenting protection visa applicants onshore at the department's Sydney and Melbourne offices.
> In April 2010, the department signed a memorandum of understanding (MOU) with the Australian Government agency CrimTrac, which provides national information-sharing solutions to law enforcement agencies. The MOU enables the department to store and match biometric data on CrimTrac's National Automated Fingerprint Identification System (NAFIS) which contains fingerprints and related information used for law enforcement purposes"[12].

In November 2012, changes to temporary work visas were made[13]. Furthermore, in July 2013, the Australian Customs and Border Protection Service (ACBPS) released a Blueprint for Reform and Australian Federal Police (AFP) Strategic Partnership 2013-2018[14].

Mexico's Immigration Policy:

The Ministry of Interior through the National Institute of Migration (INM)[15] manages the arrival, departure and settlement of migrants in Mexico. The INM is also responsible for the control and enforcement of the migratory policy.

Mexico has some of the most complex immigration dynamics in the world. Based on the criteria set by the Global Commission on International Migration (GCIM)[16] and International

[10] Idem
[11] Australia Government, Department of Immigration and Citizenship, *Annual Report* (2010-2011)
[12] Idem.
[13] http://www.immi.gov.au/visas/temporary-visa/ (20/12/2012)
[14] Australia Governments, Australian Customs and Border Protection Service, *The Blueprint for Reform* (2013-2018)
[15] Mexico, National Institute of Migration (INM) http://www.inm.gob.mx/index.php/page/pagina_principal/en.html (20/12/2012)
[16] The website points out that: *"The GCIM was launched by the United Nations Secretary-General and a number of governments in 2003. It was comprised of 19 Commissioners, was independent and was given the mandate to provide the framework for the formulation of a coherent, comprehensive and global response to the issue of international migration. In its Report, presented to UN Secretary-General Kofi Annan, UN Members States and other stakeholders on 5 October 2005, the Global Commission on International Migration says the international community has failed to realize the full potential of migration and has not risen to the many opportunities and challenges it presents. The Commission stresses the need for greater coherence, cooperation and capacity to achieve a more effective governance of international migration".* The Global Commission on International Migration closed in 2005. http://www.gcim.org/ (20/12/2012)

Organization for Migration (IOM), Mexico is classified as an origin[17], transit[18] and destination[19] country.

The flow of undocumented people from Mexico, Central and South America across the northern border to the United States continues while Mexico's southern border is increasingly used by citizens from Central and South America as their way into the United States.

> "Some 200,000 Central Americans attempt to irregularly enter the US via Mexico's southern border. Although 70 per cent of them are detained by Mexican migration authorities and returned to their countries of origin, an estimated 60,000–70,000 eventually reach the US or remain in Mexico"[20].

In July 2010, the Mexican immigration legal framework changed and took effect in May 2010. Mexico's *General Population Law*[21] sets out the rights and obligations of foreigners, as well as the different categories associated with immigration. However, the legislation did not respect the human rights of foreigners as recognised by the international legal framework. Even with this amendment, major issues continued in force, such as huge discretionary powers granted to immigration agents, gaps in immigration policy oversight from the legislature and judiciary and the omission of human rights for immigrants.

Perhaps, two cases prompted this legislative reform. In August 2010, seventy-two Central American migrants were murdered by drug cartels in the state of Tamaulipas in northern Mexico[22] and in December 2010, fifty Central American migrants disappeared in the state of Oaxaca in southern Mexico[23]. Central American governments pressured Mexican government not only to investigate the crimes, but also to recognise immigrants' human rights.

Thus, specific legislation –the *Migration Law*- was enacted on May 25, 2011 and came into force the following day[24]. A new *Refugees and Complementary Protection Law*[25] was approved in January 2011, as well as an amended *General Population Law*, all of which constitute Mexico's immigration legal framework.

---

[17] Origin countries: citizens migrate out because they are unable to benefit from safety, security or sustainable livelihoods in their own countries.

[18] Transit countries: people who are moving across their territory, on their way to another country or continent.

[19] Destination countries: migrants who have moved in a regular and irregular manner.

[20] IOM, *Migration Initiatives Appeal 2010* (2010) http://publications.iom.int/bookstore/free/Migration_Initiatives_2010.pdf (20/12/2012)

[21] *Ley General de Población, DOF 07/01/1974 [General Population Law, last amendment 09/04/12] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/140.pdf (20/12/2012)*

[22] Editorial, "Migrantes, 72 muertos de fosa en Tamaulipas" *El Universal* (Mexico), 25 August 2010 http://www.eluniversal.com.mx/notas/704017.html (20/12/2012)

[23] Editorial, "Intensifican búsqueda de migrantes desaparecidos" *La Gente* (Mexico online), 24 December 2010 http://www.rlp.com.ni/noticias/90585/intensifican-busqueda-de-migrantes-desaparecidos-en-mexico (20/12/2012)

[24] *Ley de Migración, DOF 25/052011 [Migration Law] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LMigra.pdf (20/12/2012)*

[25] *Ley sobre Refugiados y Protección Complementaria, DOF 27/01/2011* [Refugees and Complementary Protection Law] (Mexico) http://www.diputados.gob.mx/LeyesBiblio/pdf/LRPC.pdf (20/12/2012)

A programme called the Security and Prosperity Partnership (SPP) was adopted by Mexico, Canada and the United States. Its spheres of action involved the movement of people and it discussed a number of issues not covered by the North American Trade Agreement (NAFTA), like border security and antiterrorism measures, energy sector integration, environmental protection, emergency preparedness and safety standards, among others[26]. The principle of shared responsibility for immigration among sending and receiving countries was at the heart of ongoing reflection in Mexico[27]. However, in 2009, the SPP was abandoned by the U.S. government and NAFTA was renegotiated. At the same time, the U.S. government implemented the Global Online Enrolment System (GOES)[28].

For the purposes of this thesis, the sphere of action of this policy developed in a trilateral alliance between Canada, the United States and Mexico is very important. In the area of immigration, the programme specifications ranged from shared technology for registering passengers in North America, shared access to databases, special clearance for pre-cleared border residents, coordinated visas policies, exchange of intelligence information on certain persons and fast-track lanes to militarising Mexico's northern border, among others.

The new immigration policy for Mexico's southern and northern borders now focuses on proposals for an integrated immigration policy. The proposal is made up of four strategic lines developed by the Mexican National Institute of Migration and the Secretary of Foreign Affairs, with the cooperation of IOM[29]:

- *The facilitation of documented migration flows whose temporary or final destination is the State along Mexico's border.* The main objectives are to facilitate the documentation and entry of temporary workers and local visitors, tourists and business travellers across the border, fostering the use of migration documents and the dissemination of their benefits.

- *The protection of the rights of immigrants entering through Mexico's border.* The specific objectives of this type of protection include intensifying personnel training; supervising migrant rights during their holding, lodging and repatriation; timely treatment of cases of migrant rights violations; legal protection of migrants who are victims of trafficking or smuggling; better coordination of the authorities corresponding to migrant rights and stronger protection of the rights of refugees, asylum seekers and stateless individuals.

[26] The SPP was opened on March 23, 2005, when the leaders of the United States, Canada and Mexico met in Waco, Texas.
[27] Security and Prosperity Partnership of North America (SPP) http://www.spp-psp.gc.ca/eic/site/spp-psp.nsf/eng/home (20/12/2012)
[28] https://goes-app.cbp.dhs.gov/main/goes (20/12/2012) This includes the FAST Driver Programme between the United States and Canada or the United States and Mexico. FAST is the trusted traveller programme for commercial truck drivers along Canadian and Mexican land borders. FAST allows for the expedited release of approved commercial truck drivers making fully-qualified FAST trips between the United States and either Canada or Mexico. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/fast/ (20/12/2012)
[29] OECD, *Recent changes in Migration Movements and Policies: Country Notes* (2010), p. 198; see also IOM, *Migration initiatives 2012* (2012), p. 61 http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/published_docs/books/Migration-Initiatives-Appeal.pdf#australia (20/12/2012)

- *Contribution to border security*. The main actions are to reinforce immigration control and the verification of a foreigner's legal stay in Mexico; to fight trafficking and people smuggling in coordination with other institutions, especially where women and minors are involved; to provide better information exchange between the institutions involved in combating criminal activities and to take measures to stop corruption among immigration authorities.

- *The permanent updating of immigration flow management and legislation in order better to handle the changing dynamics of immigration on the border*. The objectives include the modernisation of the infrastructure for registering and controlling migration flows; the implementation of specific mechanisms for collecting and analysing information for decision-making; the evaluation of programmes, projects and actions to obtain appropriate feedback; and the adaptation of legislation in the light of the changing dynamics of migration in the region.

There are two main classifications of migratory criteria to legally enter Mexico: as a visitor and as a resident (temporary or permanent)[30]. As a visitor, there are seven subclasses of visa: visitor as tourist, in transit, visitor as businesspeople or investors, visitor for the adoption of minors, visitor as a cross-border worker, visitor for humanitarian reasons and visitor as regional resident; whereas there are three subclasses of residents: temporary resident as a student, temporary resident and permanent resident.

Neither Mexico's *General Population Law* nor *Migration Law* consider the implementation of biometric systems. However, the implementation of biometric systems is established in the *Manual of Criteria and Migratory Proceedings of the National Institute of Migration.* This document is not updated because it has the old classifications of visas, but the rest of the document is still applicable to biometric systems in the following cases[31].

a) Foreign holders of a valid visa who want to change their status in Mexico as temporary residence or permanent residence; also it applies for that they wish to replace its migratory form by robbery, lost or partial destruction[32]
b) Refugee (humanitarian and asylum reasons)[33]
c) Temporary and definitive Asia Pacific Business Travel Card (ABTC)[34]

These three biometric lists belong to the new immigration procedures deployed as a centralised information system called the Electronic System for Migration Procedures (SETRAM)[35].

---

[30] *Ley de Migración, DOF 25/052011 [Migration Law] (Mexico)*, above n 115.
[31] *Acuerdo por el que se expide el Manual de Criterios y Trámites Migratorios del Instituto Nacional de Migración, DOF 29/01/2010, [Criteria and Migratory Proceedings Manual of the National Institute of Migration of the Minister of Interior of 21 September 2010] (Mexico)* http://dof.gob.mx/nota_detalle.php?codigo=5129775&fecha=29/01/2010 *(20/12/2012)*
[32] As a safeguard for foreigners' the immigration shall issue them migratory forms with biometric elements of security in agreement with the administrative norms.
[33] The National Institute of Migration will issue proof of the request of recognition of the condition of Refugee. This proof shall state that the request is under review and will also contain the applicant's personal data and biometric information. The same shall apply to the dependants who accompany the applicant.
[34] The ABTC temporary will be issued when the answer of a member economy is unresolved and the applicant wishes to enter the member economies that have already approved the request; the ABTC definitive will be issued when all member economies have been pronounced on the request of the Mexican authority approving or denying the expedition of the card.

The INM also launched the interconnection of the Integrated Migration Operations (SIOM by its Spanish acronym) with the INM's Electronic Immigration Procedures (SETRAM by its Spanish acronym), the Consular Management Integrated System (ACIS by its Spanish acronym) of the Ministry of Foreign Affairs (SRE by its Spanish acronym). This interconnection allows Mexican consulates to automatically verify migration real-time alerts at the time of issuing visas, in order to assess the issuance of the type of visa requested. The INM also informs the SRE of the permits granted to foreigners to obtain their visas at the corresponding consulates[36].

New Zealand's Immigration Policy:

The Department of Labour manages migration flows and border security. However, the Department of Internal Affairs (Citizenship Branch), Electoral Enrolment Centre and Department of Internal Affairs (Births, Deaths and Marriages) are authorised to provide better services to perspective immigrants[37]. Immigration is fundamental to New Zealand's economy. The *Immigration Act 2009* came into effect in November 2010. The new immigration policy has three main objectives: economic transformation, strong national identity and security, and opportunity for families[38].

The new Act allows for the following types of visas: residence class visas and temporary entry class visas. There are two residence class visas: resident visa and permanent residence visa. There are four temporary entry class visas: temporary visas, limited visas, interim visas and transit visas. However, there are a variety of temporary visas. The new Act has modernised New Zealand's immigration laws, but *"it does not make major changes to the criteria under which people apply to travel to and stay in New Zealand"*[39].

In 2009, the SmartGate was implemented at Auckland International Airport for arriving passengers from Australia and New Zealand. It is also operational for departing passengers from Australia and New Zealand at the Auckland, Wellington and Christchurch international airports[40].

The *2009 Immigration Act* allows for the collection of biometric information from foreign nationals and New Zealand citizens on arrival in New Zealand for immediate use and storage for future use: photographs of all or part of a person's head or shoulders, fingerprints and iris scans. However, for New Zealand citizens, the biometric data will be matched against the information in their New Zealand passport. Once the person's identity and citizenship is confirmed, the information is disposed of and is not stored.

---

[35] Mexican Government, National Institute of Migration, *Action Lines in Sector Programs Accountability, Transparency and Fighting Corruption committed in 2009* Final Report (2008-2012) http://www.inm.gob.mx/static/transparencia/PND/Formatos_A_y_B.pdf (20/12/2012)

[36] Instituto Nacional de Migración, "Consolida INM simplificación de trámites migratorios", (Press Release, 7 September 2011) http://www.inm.gob.mx/index.php/blog/show/Consolida-INM-simplificaci%C3%B3n-de-tr%C3%A1mites-migratorios.html (22/12/2012)

[37] New Zealand immigration area of responsibility http://www.dol.govt.nz/about/responsibilities/ (22/12/2012)

[38] New Zealand Government, *Immigration Act Review* (April 2006)

[39] *Immigration Act 2009* (New Zealand), see also the following website: http://www.immigration.govt.nz/migra/general/generalinformation/immigrationact/ (20/12/2012)

[40] New Zealand, Customs Service website http://www.customs.govt.nz/features/bordersector/transtasmantravel/Pages/default.aspx (20/12/2012)

In 2012, New Zealand started to introduce a new online immigration system to process visas applications called Immigration Global Management System (IGMS)[41].

Spain's Migration Policy:

Spain is classified as a transit and destination country. The Minister of Labour and Migration by the Secretary of Migration and Immigration manage the arrival and settlement of migrants[42].

From 2000 to 2009, Spain has amended its legal framework on migration. The most recent amendments were carried out in 2007 and 2009: *The 2/2009 Organic Law which reforms the Organic Law 4/2000 on Rights and Liberties for Foreigners in Spain and their Social Integration*[43] and *Royal Decree 1161/2009 which reforms Royal Decree 240/2007 on the Arrival, Free Flow and Residence for European Citizens in Spain, Members of the European Union and Schengen Agreement*[44]*.* The second reform marks the beginning of a new stage in Spanish policy that is the result of the change not only of the political party in power's perspective on this matter, but also of the dispositions established in the Treaty of Amsterdam and the agreements adopted at the Tampere and Seville Summits aiming at the formulation of a common policy in flow control and the allocation of rights of immigrant-based communities.

These reforms were part of a comprehensive and coordinated approach in handling migration in Spain, which provides a broad view of all the aspects and not only from a single perspective like that of control flow, the integration of foreign residents or the development of countries of origin.

The Spanish population has increased because European Union nationals do not need to apply for a residence permit[45]. Current legislation on immigration promotes the integration of immigrants already living in Spain and strengthens the controls and sanctions in the field of undocumented immigration and the illegal employment of foreigners. *The Organic Law 4/2000 on the Rights and Liberties for Foreigners in Spain and their Social Integration* sets two main visa categories: Stays and Residence. The first one has seven different types of visas and the second has two classifications: temporary and permanent residence[46]. Even though this legislation has been amended, the visa categories are applicable.

---

[41] New Zealand, New IT System for Immigration New Zealand http://www.immigration.govt.nz/migrant/general/generalinformation/newitsystems/ (20/12/2012)

[42] Spain, General Minister for Migration and Immigration http://extranjeros.mtin.es/es/Organizacion/ (20/12/2012)

[43] *Ley Orgánica 2/2009, de 11 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social,BOE-A-2009-19949 [Organic Law 2/2009 amending Organic Law 4/200 on the Rights and Liberties for Foreigners in Spain and their Social Integration] (Spain), http://www.boe.es/buscar/doc.php?id=BOE-A-2009-19949 (20/12/2012)*

[44] *Real Decreto 1161/2009, de 10 de julio, por el que se modifica el Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España de ciudadanos de los Estados miembros de la Unión Europea y de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo, BOE-A-2007-4184, [Royal Decree on the Entry, Free Movement and Residence in Spain of Citizens of the Member States of the European Union and Other States Party to the Agreement on the European Economic Area] (Spain) http://www.boe.es/buscar/doc.php?id=BOE-A-2007-4184 (20/12/2012)*

[45] However, they should hold a Foreign ID Card issued by the European Union agreements.

[46] Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, BOE-A-2000-544 [*Organic Law 4/2000 on the Rights and Liberties for*

The Spanish migration policy is focused on undocumented immigration and the integration of immigrants legally residing in Spain. To implement this policy, controls are carried out both when immigrants enter the country and when they take up residence. Carriers are now responsible for verifying the legality of the documents shown to them under pain of sanctions. They are also required to inform the authorities of any unused return tickets. Lastly, municipalities are required to keep their registers up-to-date so as to ensure that the data are consistent with residence permit data[47].

Foreigners in Spain and their Social Integration] (Spain) http://www.boe.es/buscar/act.php?id=BOE-A-2000-544 (20/12/2012)

[47] OECD, *Recent Changes in Migration Movements and Policies: Country Notes* (2010), above n 117 and see also IOM, *Migration Initiatives 2012* (2012), above n 117.

APPENDIX I.

FOUR COUNTRIES PRIVACY REGIME (COMPARATIVE TABLE)

Comparative Privacy and Data Protection Laws		
Country	**Title**	**Definitions**
		Personal Data
Australia	Privacy Act 1988	***Personal information*** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, form the information or opinion. ***Sensitive information*** means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinion: or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; r (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information.
Mexico	Federal Transparency and Access to Governmental Public Information Act	***Personal data*** any information concerning an identified or identifiable a natural person (individual) ***Personal data system***: Systematized personal data in the possession of a disclosing party
New Zealand	Privacy Act 1993	***Personal information*** means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act ***Unique identifier means*** an identifier- (a) that is assigned to an individual by an agency for the purposes of the operations of the agency; and (b) that uniquely identifies that individual in relation to that agency;- but, for the avoidance of doubt, does not include an individual's name used to identify that individual
Spain	Organic Law15/1999 of 13 December on the Protection of Personal Data	***Personal data:*** any information concerning identified or identifiable natural persons. ***Processing of data:*** operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and cancellation, as well as assignments of data resulting from communications, consultations, interconnections and transfers.

Country	Functions of Commissioners
Australia	To investigate an act or practice of an agency To approve privacy codes To investigate an act or practice of an organisation To perform functions, and exercise powers, conferred on an adjudicator by an approved privacy code To review the operation of approved privacy codes To review the determination of an adjudicator in relation to a complaint To examine a proposed enactment that would require or authorise acts or practices of an agency or organisation. To undertake research into, and to monitor developments in, data processing and computer technology (including data-matching and data-linkage) To promote an understanding and acceptance of the Information Privacy Principles To prepare, and to publish guidelines for the avoidance of acts or practices or an agency or an organisation To provide advice to a Minister To provide advice to an adjudicator To maintain, and to publish annually, a record of the matters set out in records maintained by record-keepers To conduct audits of records of personal information To examine a proposal for data matching or data linkage that may involve an interference with the privacy of individuals For the purpose of promoting the protection of individual privacy, to undertake educational programs on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner To issue guidelines To monitor and report on the adequacy of equipment and user safeguards May, and if requested to do so, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interest of the privacy of individuals
Mexico	To interpret this Act in the administrative sphere in terms of Article 6. To hear and issue a ruling on the writs of review filed by applicants; To design and review the criteria for classification, declassification and custody of privileged and confidential information; To act as coadjutant of the National Archives in the preparation and application of criteria for listing and keeping of documents, and for the organization of department and agency files. To supervise, and in case of non-performance, issue recommendations to the departments and agencies for the enforcement of the provisions of Article 7 herein; To provide counselling to private entities about their requests for access to information; To provide technical support to departments and agencies in the formulation and implementation of their information programs in terms of Article 29, section VI, herein; To design the forms for the requests for access to information, as well as the forms for access to and correction of personal data. To set forth the general guidelines and policies for the handling, maintenance, safety and protection of the personal data kept by departments and agencies;

	Under the terms of Article 56, last paragraph herein, to inform the internal control body of each department and agency of the alleged infringement of this Act and its Regulations. The resolution issued to the effect by internal control bodies shall be final and conclusive and shall be notified to the Institute for publication in its annual report; To formulate the guidelines consigned in Article 38 herein. To promote and, if applicable, carry out the training of government officials in the access to information and personal data protection. To disseminate among government officials and private entities the benefits of public handling of information, as well as their responsibility in the sensible use and preservation thereof; To prepare and publish studies and research to disseminate the knowledge on the subject matter of this Act; To cooperate in connection with this Act with the other disclosing parties, states, municipalities and their bodies, giving access to information through the execution of agreements or the implementation of programs; To prepare its Internal Regulations, as well as any other operating directives; To designate the government officials to be in charge of the Institute; To prepare its annual budget plan to be submitted to the Department of Finance and Public Credit for inclusion in the Federal Budget, and Any other attributions conferred thereto by this Act, its Regulations or any other applicable provision.
New Zealand	To promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the object of those principles to conduct an audit of personal information maintained by an agency To monitor the use of unique identifiers and to report to the Prime Minster To maintain and to publish directories of personal information To monitor compliance with the public register privacy principles To examine any proposed legislation that makes provision for collection or/and disclosure of personal information For the purpose of promoting the protection of individual privacy, to undertake educational programmes To make public statements into, and monitor developments in , data processing and computer technology To examine any proposed legislation or proposed policy of the government To report to the Prime Minister To publish reports relating generally to the exercise of the Commissioner's functions
Spain	To ensure compliance with the legislation on data protection and ensure its application, in particular as regards the rights of information, access, rectification, objection and cancellation of data. To issue the authorisations provided for in the Law or in its regulatory provisions. To issue, where applicable, and without prejudice to the remittances of other bodies, the instructions needed to bring processing operations into line with the principles of this Law. To consider the applications and complaints from the data subjects. To provide information to persons on their rights as regards the processing of personal data. To require controllers and processors, after having heard them, to take the necessary measures to align the processing operations with this Law and, where applicable, to order the cessation of the processing operation, when the operation does not comply with the

	provisions of the Law. To impose the penalties set forth in Title VII of this Law. To provide regular information on the draft general provisions set forth in this Law. To obtain from the data controllers any assistance and information it deems necessary for the exercise of its functions. To make known the existence of personal data files, to which end it shall regularly publish a list of such files with any additional information the Director of the Agency may deem necessary. The decisions of the Spanish Agency of Data Protection shall be made public once they are notified to interested parties. The publication will be made preferably through media or telecommunications. Regulations may establish the terms under which it carries out the dissemination of those resolutions. The provisions of the preceding paragraphs shall not apply to decisions relating to the registration of a data controller in the General Registry of Data Protection or those for which registration is resolved in the same type of code is governed by Article 32 of this Act.

Country	Principles
Australia	Manner and purpose of collection of personal information Solicitation of personal information from individual concerned Solicitation of personal information generally Storage and security of personal information Information relating to records kept by record-keeper Access to records containing personal information Alteration of records containing personal information Record-keeper to check accuracy etc. of personal information before use Personal information to be used only for relevant purposes Limits on use of personal information Limits on disclosure of personal information
Mexico	To implement the procedures required to receive and resolve the requests for accessing and correcting data, to train government officials and provide information on their policies in connection with the protection of mentioned data under terms of the guidelines issued by the Institute or the equivalent bodies consigned in Article 61 herein; to handle the personal data as long as deemed adequate, appropriate and moderated in connection with the purposes for which they were obtained; to make a document available to private entities, at the time of obtaining personal data, stating the purposes for its treatment, under the terms of the guidelines issued by the Institute or the equivalent body stipulated in Article 61; to do their best so that the personal data are accurate and updated; to substitute, correct or complete, on a mandatory basis, personal data that are inaccurate in full or in part, or incomplete, as soon as the disclosing parties are aware of this situation; to implement the required measures to warrant the safety of personal data and prevent their alteration, loss, transfer or unauthorized access.
New Zealand	Purpose of collection of personal information Source of personal information Collection of information from subject Manner of collection of personal information Storage and security of personal information Access to personal information Correction of personal information Accuracy, etc, of personal information to be checked before use Agency not to keep personal information for longer than necessary Limits on use of personal information Limits on disclosure of personal information Unique identifiers
Spain	Quality of the data Right of information in the collection of data

	Consent of the data subject Data with special protection Data on health Data security Duty of secrecy Communication of data Access to data on behalf of third parties Right of access Right of rectification or cancellation

APPENDIX J.

INTERVIEW QUESTIONS AND INTERVIEWEES

Note: This semi-structured face-to-face interviews with academics and public officials in the four countries study are part of the empirical methodology employed in the study and were introduced through all the body of the thesis and has been cross referenced in the body of this thesis. This component of the research project received approval from the University of Tasmania Human Research Ethics Committee. Approval Ethics Ref: H0012013 of 29/08/2011

1. *Existing biometric systems (databases)*
   1.1. What biometric systems are being used in your country?
   Please look at the attached chart. I have identified a number of biometric systems operating in your country.
   1.2. Do you know of other databases in your country?
   1.3. Has the use of biometric systems increased in your country?

2. *Policies for development of databases.*
   2.1. What policies accompanied the introduction of biometrics in your country?
   2.2. Are these policies publicly available?
   2.3. What were the reasons and purposes for introducing biometric systems in your country?
   2.4. Are you aware of any plans for the expansion of biometric databases?

3. *Data protection and exchange information*
   3.1. What are the specific rules or standards on data protection for biometric information collection in your country?
   3.2. Is the biometric data that you collect exchangeable with any other national or international organisation and, if so under what conditions?
   3.3. Does your organisation have special rules for the exchange of information based on security reasons, particularly terrorism?

4. *Access to personal information.*
   4.1. How can a person find out whether biometric data is held by a national authority and how can this information be verified and/or corrected?
   4.2. Was any consultation process undertaken before the implementation of biometric systems?
   4.3. Do you have any guide for exercising the right of access to information on databases and explaining the procedure for such a request?
   4.4. Do you believe that your organisation provides sufficient public information about biometric systems?

5. *Future directions.*
   5.1. What are the socio political and ethical issues in relation to biometric systems?
   5.2. Are any new mechanisms for governance of biometric systems proposed in your country?
   5.3. In what other areas do you think that biometric systems, as a mechanism of surveillance, will be used in the future?
   5.4. Is biometric technology spreading in your society?

The following people were interviewed:

Australia:

- Jeremy Johnson, Director National Biometric and Child Protection Services, CrimTrac Agency (Canberra, 18 October 2011)
- Alex Webling, Policy Director, Biometrics and Identity, Attorney General's Department (Canberra, 20 October 2011)
- Charlotte Epstein, Professor, University of Sydney (Sydney, 28 October 2011)
- Katina Michael, Associate Professor, University of Wollongong (Sydney, 21 February 2012)

Mexico:

- Lina Ornelas, General Director of Self-Regulation, Instituto Federal de Acceso a la Información y Protección de Datos [Federal Access Information and Data Protection Institute] (Mexico City, 15 November 2011)
- Alejandro del Conde, Secretary of Data Protection, Instituto Federal de Acceso a la Información y Protección de Datos [Federal Access Information and Data Protection Institute] (Mexico City, 16 November 2011)
- Ernesto Villanueva Villanueva, Professor, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [Legal Research Centre of the National Autonomous University of Mexico] (Mexico City, 23 November 2011)
- Issa Luna Pla, Professor, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [Legal Research Centre of the National Autonomous University of Mexico] (Mexico City, 23 November 2011)
- Alberto Arellano Méndez, Researcher, Instituto Nacional de Medicina Genomica [National Institute of Genomic Medicine] (Mexico City, 23 November 2011)

New Zealand:

- David Philp, General Manager-Passport, Department of Internal Affairs (Wellington, 25 October 2011)

Spain:

- Francisco Villanueva Díez, Deputy General Director of Information Systems and Communications for Security Matters, Spanish Minister of Interior (Madrid, 8 November 2011)
- Pilar Nicolás Jiménez, Professor, University of Deusto (Bilbao, 10 November 2011)

APPENDIX K.

LEGISLATION OF BIOMETRIC IDENTIFIER NEW JERSEY

In 2002, the State of New Jersey introduced the Biometric Identifier Privacy Act:
Be It Enacted by the Senate and General Assembly of the State of New Jersey:
1. This act shall be known and may be cited as the "Biometric Identifier Privacy Act.
2. As used in this act:
"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of a hand or a face geometry.
"Governmental entity" means the State, any agency, authority, or employee thereof, or any political subdivision of the State, including but not limited to any county, municipality, or school district, or any agency, authority, or employee thereof.
3. a. Notwithstanding any other provision of law to the contrary, no person shall obtain a biometric identifier of an individual, for the purpose of commercial advantage, without authorization of the individual.
b. A person who possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier to another person unless:
(1) The individual consents to the sale, lease or disclosure;
(2) The sale, lease or disclosure completes a financial transaction requested or authorized by the individual;
(3) The sale, lease or disclosure is required or permitted by federal or State law; or
(4) The sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose.
c. A person who possesses a biometric identifier of an individual shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects other confidential information.
d. A person aggrieved by a violation of this section may bring an action in the Superior Court to enjoin further violation and to recover for the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.
e. Any person who violates any provision of this section shall be liable for a civil penalty of not more than $25,000 for each violation. Any such penalty shall be enforced and collected in accordance with "The Penalty Enforcement Law of 1999," P.L.1999, c.274 (C.2A:58-10 et seq.). Any action to collect or enforce any such penalty shall be brought in the Superior Court by the Attorney General or county prosecutor.
4. a. A governmental entity that possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier to another person unless:
(1) the individual consents to the sale, lease or disclosure;
(2) the sale, lease or disclosure is required or permitted by a federal or State law; or
(3) the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose.
b. A governmental entity that possesses a biometric identifier of an individual shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental entity stores, transmits, and protects other confidential information.
c. A governmental entity that possesses a biometric identifier of an individual shall establish a reasonable procedure under which an individual is entitled to have the governmental entity correct information about the individual that is possessed by the governmental entity and that is incorrect. The procedure shall not unduly burden an individual using the procedure.

d. A person aggrieved by a violation of this section may bring an action in the Superior Court, to enjoin further violation and to recover the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.
e. Information compiled pursuant to this section shall not be subject to disclosure pursuant to P.L.1963, c. 73 (C.47:1A-1 et seq.) as amended and supplemented.
5. This act shall take effect immediately.
STATEMENT
This bill, the "Biometric Identifier Privacy Act," provides guidelines for the use and distribution of biometric identifiers and establishes civil penalties for the misuse of the information.
A biometric identifier is a retina or iris scan, fingerprint, voiceprint, or record of a hand or a face geometry. Biometrics technology is a non-invasive method of using computer technology to provide automatic identification or identity verification or authentication of individuals. The technology acquires an image of a physical feature which is then applied to the algorithm to produce a "template." This "template" is then encrypted for data transmission and storage. This stored "template" can then be stored and compared against the live "template" when necessary. This technology is being used for criminal identification as well as in airport security systems, border clearances and for transaction verifications in internet businesses. It is the sponsor's intent to protect the users of this technology by insuring that this data is not obtained, disclosed, misused or released without an individual's authorization.
Under the provisions of the bill a person cannot obtain another individual's biometric identifier information, for the purpose of commercial advantage, without authorization from that individual. The bill prohibits a person who possesses a biometric identifier of another individual from selling, leasing, or otherwise disclosing this information unless: the individual consents to the sale, lease or disclosure; the sale, lease or disclosure completes a financial transaction requested or authorized by the individual; the sale, lease or disclosure is required or permitted by federal or State law; or the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose. A person who possesses a biometric identifier of an individual would be required to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which that person stores, transmits, and protects other confidential information. The bill provides that any person who violates the provisions of the act would be liable for a civil penalty of not more than $25,000 for each violation. The Attorney General or county prosecutor would bring the action to collect or enforce the penalty in Superior Court. Furthermore, the bill provides that any person who has been aggrieved by a violation of the act may bring an action in the Superior Court, to enjoin further violation and to recover the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.
In addition, the bill prohibits any governmental entity which possesses a biometric identifier of an individual from selling, leasing, or otherwise disclosing the biometric identifier to another person unless: the individual consents to the sale, lease or disclosure; the sale, lease or disclosure is required or permitted by a federal or State law; or the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose. A governmental entity that possesses a biometric identifier of an individual would be required to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental entity stores, transmits, and protects its other confidential information. The bill also requires the governmental entity to establish a reasonable procedure under which an individual is entitled to have the governmental entity correct information about the individual that is possessed by the governmental entity and that is incorrect. The procedure cannot be unduly burdensome.

APPENDIX L.

LEGISLATION OF BIOMETRIC INFORMATION ILLINOIS.

In 2008, the State of Illinois introduced the Biometric Information Privacy Act:
(740 ILCS 14/1)
Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/5)
Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:
(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.
(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.
(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.
(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.
(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.
(f) The full ramifications of biometric technology are not fully known.
(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/10)
Sec. 10. Definitions. In this Act:
"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.
"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.
"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.
"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/15)
Sec. 15. Retention; collection; disclosure; destruction.
(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.
(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.
(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.
(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.
(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/20)
Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:
(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
(4) other relief, including an injunction, as the State or federal court may deem appropriate.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/25)
Sec. 25. Construction.
(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.
(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.
(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.
(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated there under.
(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/30)
Sec. 30. (Repealed).
(Source: P.A. 95-994, eff. 10-3-08. Repealed internally, eff. 1-1-09.)
(740 ILCS 14/99)
Sec. 99. Effective date. This Act takes effect upon becoming law.
(Source: P.A. 95-994, eff. 10-3-08.)

APPENDIX M.

LEGISLATION OF ONTARIO, CANADA

Works Act-Statutes of Ontario 1997, Canada

Ontario Works Act-Statutes of Ontario 1997, c 25
Biometric information
75. (1) Where this Act or the regulations authorize a person to collect or use personal information, biometric information may be collected or used only for the following purposes:
1. To ensure that an individual is registered only once as an applicant, recipient, spouse or dependent adult.
2. To authenticate the identity of an individual who claims to be entitled to assistance.
3. To enable an individual to receive and give receipt for assistance provided through a financial institution or other authorized provider.
4. To enable an applicant, recipient, spouse or dependent adult to access personal information.
5. To enable an individual to make a declaration electronically by voice or other means for any purposes authorized under this Act.
6. To match data in accordance with an agreement made under section 71 or 72 for the purpose of ensuring eligibility for assistance or benefits. 1997, c. 25, Sched. A, s. 75 (1); 1999, c. 6, s. 50 (7); 2005, c. 5, s. 54 (7).
(2) Biometric information may be collected under this Act only from the individual to whom it relates, in accordance with an agreement referred to in paragraph 6 of subsection (1) or in accordance with section 73.
(3) Biometric information shall not be disclosed to a third party except in accordance with,
(a) a court order or a warrant;
(b) an agreement under section 71 or 72 that is made for the purpose of ensuring eligibility for a social benefit program, including a social benefit program under the Income Tax Act, the Taxation Act, 2007 or the Income Tax Act (Canada); or
(c) section 73.
(4) Biometric information to be collected from the individual to whom it relates shall be collected openly and directly from the individual.
(5) An administrator shall ensure that biometric information can be accessed and used only by those persons who need the information in order to perform their duties under this Act and that it is not used as a unique file identifier or common personal file identifier, except as authorized under subsection (1).
(6) An administrator shall ensure that biometric information collected under this Act is encrypted forthwith after collection, that the original biometric information is destroyed after encryption and that the encrypted biometric information is stored or transmitted only in encrypted form and destroyed in the prescribed manner.
(7) Neither the Director nor an administrator shall implement a system that can reconstruct or retain the original biometric sample from encrypted biometric information or that can compare it to a copy or reproduction of biometric information not obtained directly from the individual.
(8) The only personal information that may be retained together with biometric information concerning an individual is the individual's name, address, date of birth and sex.
(9) For the purpose of section 67 of the Freedom of Information and Protection of Privacy Act and section 53 of the Municipal Freedom of Information and Protection of Privacy Act, subsection (3) is a confidentiality provision that prevails over those Acts.